MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

Paul T. McGurkin, Jr.
Office: 267-930-4788
Fax: 267-930-4771
Email: pmcgurkin@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

July 12, 2019

VIA U.S. MAIL

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

Re: Notice of Data Security Incident

Dear Attorney General MacDonald:

We represent Oberlin College ("Oberlin"), 38 East College Street, Oberlin, OH 44074, and are writing to notify you of a recent incident that may affect the security of the personal information of certain New Hampshire residents. The investigation into this event is ongoing, and this notice may be supplemented if significant facts are learned subsequent to its submission. By providing this notice, Oberlin does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

Nature of the Data Security Incident

On or about March 5, 2019, Oberlin learned of suspicious activity occurring within its admissions software. Oberlin immediately conducted an internal investigation and determined that an unauthorized actor gained access to sensitive data relating to certain current and prospective students. Oberlin provided preliminary notice of this event via email to impacted individuals on March 7, 2019. Oberlin provided a second preliminary notice to these individuals between March 20, 2019 and March 30, 2019 which included an offer of 12 months of complimentary credit monitoring.

A forensic investigator was engaged to determine what happened and what information was involved. The investigation confirmed that an unauthorized actor gained access to certain records held in Oberlin's network on March 5, 2019. On June 8, 2019, Oberlin completed the review of the records subject to unauthorized access and confirmed the identities of those individuals who were impacted by this event. Through this review, Oberlin determined that personal information relating to New Hampshire residents was potentially affected.

The investigation determined the names and Social Security numbers relating to twelve (12) New Hampshire residents were impacted in relation to this incident.

Notice to New Hampshire Residents

Oberlin provided written notice of this incident to twelve (12) New Hampshire residents on July 12, 2019, in substantially the same form as the letter attached hereto as ***Exhibit A***.

Other Steps Taken and To Be Taken

Oberlin takes this incident and the security of personal information in its software seriously. Upon discovery of this incident, Oberlin immediately took steps to secure the software and launched an in-depth investigation with the assistance of a third-party forensic investigation firm to determine the nature and scope of this incident. Additionally, Oberlin provided information to the FBI regarding this incident. As part of Oberlin's ongoing commitment to the privacy of personal information in its care, it reviewed its existing policies and procedures and implemented additional safeguards to further secure the information in its systems. Oberlin is also notifying regulatory authorities, as required by law.

Oberlin is providing potentially affected individuals access to twelve (12) months of credit monitoring and identity restoration services through TransUnion. Additionally, Oberlin is providing potentially impacted individuals with guidance on how to better protect against identity theft and fraud, including information on how to place a fraud alert and security freeze on one's credit file, 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 identity theft and fraud 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 incident, please contact me at (267) 930-4788.

Very truly yours,

Paul McGurkin of
MULLEN COUGHLIN LLC

PTM/vfr
Enclosure

EXHIBIT A

OBERLIN

COLLEGE & CONSERVATORY

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>>

Re: Notice of Data Breach

Dear <<Name 1>>:

Oberlin College ("Oberlin") is writing to follow up with you regarding a recent event that may impact the privacy of some of your personal information. We wanted to provide you with additional information about the event, our response, and steps you may take to better protect against the possibility of identity theft and fraud, should you feel it necessary to do so. **This is not a notice of a new data event.**

What Happened?
On or about March 5, 2019, Oberlin learned of suspicious activity occurring within its admissions software. Oberlin immediately conducted an internal investigation and determined that an unauthorized actor gained access to sensitive data relating to certain current and prospective students. Oberlin notified you via email of this event. Oberlin engaged a third-party forensic investigation firm to assist with the investigation into what happened and to determine what information was affected. The investigation confirmed that an unauthorized actor gained access to certain records held in Oberlin's network on March 5, 2019. On June 8, 2019, Oberlin confirmed the identities of those individuals who were impacted by this event.

What Information Was Involved? The following information was accessed within the impacted software: your name and <<Variable Data Elements>>. To date, the investigation found no evidence that any of this information has been subject to actual or attempted misuse.

What We Are Doing. Oberlin takes this incident and the security of personal information on its software seriously. Upon discovery of this incident, Oberlin immediately took steps to secure the software and launched an in-depth investigation with the assistance of a third-party forensic investigation firm to determine the nature and scope of this incident. As part of Oberlin's ongoing commitment to the privacy of personal information in its care, it reviewed its existing policies and procedures and implemented additional safeguards to further secure the information in its systems. Oberlin is also notifying regulatory authorities, as required by law.

As an added precaution, Oberlin has arranged for you to enroll, at no cost to you, in an online credit monitoring service, *my*TrueIdentity, for 12 months provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies. Individuals who wish to receive these services must enroll by following the enrollment instructions below.

What You Can Do. You can find out more about how to protect against potential identity theft and fraud in the enclosed *Steps You Can Take to Protect Against Identity Theft and Fraud.* There you will also find more information on the credit monitoring services we are offering and how to enroll.

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 (440) 775-8755, Monday through Friday from 9:00 a.m. to 4:30 p.m. ET. You may also write to Oberlin at dataresponse@oberlin.edu.

We sincerely regret any inconvenience or concern this incident may have caused.

Sincerely,

Manuel Carballo
Vice President and Dean of Admissions and Financial Aid
Oberlin College

Steps You Can Take to Protect Against Identity Theft and Fraud

To enroll in online credit monitoring via *my*TrueIdentity, please follow the steps below:

1) Visit www.mytrueidentity.com to enroll.
2) In the space referenced as "Enter Activation Code," enter the following 12-letter Activation Code << 12- letter Activation Code>> and follow the three steps to receive your credit monitoring service online within minutes.
3) You have until <<Enrollment Date>> to activate your identity monitoring services. **Your code will not work after this date.**

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 following 6-digit telephone pass code << 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.

The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised to help you restore your identity and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.) The identity restoration assistance is available to you through July 10, 2020, with no enrollment required. If you believe you may be a victim of identity theft, please call the TransUnion Fraud Response Services toll-free hotline at 1-855-288-5422. When prompted, enter the following 6-digit telephone pass code <<6-digit Pass Code>> to speak to a dedicated TransUnion representative about your identity theft issue.

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your 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
PO Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion
P.O. Box 2000
Chester, PA 19016
1-888-909-8872
www.transunion.com/credit-freeze

Equifax
PO Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
www.equifax.com/personal/credit-report-services

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 2002
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
www.transunion.com/fraud-victim-resource/place-fraud-alert

Equifax
P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008
www.equifax.com/personal/credit-report-services

Although we have no reason to believe that your personal information has been used to file fraudulent tax returns, you can contact the IRS at www.irs.gov/Individuals/Identity-Protection for helpful information and guidance on steps you can take to address a fraudulent tax return filed in your name and what to do if you become the victim of such fraud. You can also visit www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft for more information.

If you identify any fraudulent or suspicious charges on your credit or debit card, you should immediately contact your bank or financial institution. It is also a good practice to remain vigilant of unsolicited communications seeking your credit card or other financial information. Incidents of identity theft should also be reported to your local law enforcement.

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 North Carolina residents, 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 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 Mexico residents**, you have* rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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.