MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

Christopher J. DiIenno
Office: 267-930-4775
Fax: 267-930-4771
Email: cdiienno@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

April 18, 2019

VIA U.S. MAIL

Attorney General Gordon J. MacDonald
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Security Incident

Dear Attorney General Gordon J. MacDonald:

We represent Oregon Institute of Technology ("Oregon Tech") located at 3201 Campus Drive, Klamath Falls, Oregon 97601 and write to notify your office of an incident that may affect the security of some personal information relating to one (1) New Hampshire resident. 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, Oregon Tech 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 October 25, 2018, Oregon Tech began noticing issues with its network. Oregon Tech immediately began an internal investigation into the activity and discovered that multiple systems were infected with a virus. This investigation included working with third-party forensic investigators to confirm the nature and scope of this incident. On November 16, 2018, the investigation determined that there may have been unauthorized access to certain systems between October 19, 2018 through October 23, 2018. This investigation was unable to determine what information, if any, was accessed within those systems.

Oregon Tech then initiated another investigation, to review the potentially affected systems to determine if there was any personal information present on those systems at the time of the incident. This review required an extensive systematic and manual review of the files and documents stored on the potentially affected systems. On March 3, 2019, Oregon Tech concluded this review and determined that personal information was present on the relevant systems at the time of the incident including individuals' name, address and Social Security number. Since that time, Oregon Tech has been diligently reviewing this information and its records for purposes of disclosing this incident to potentially affected individuals. To date, Oregon Tech's investigation has not revealed evidence of actual or attempted misuse of personal information as a result of this incident.

Notice to New Hampshire Resident

On April 18, 2019, Oregon Tech will begin providing written notice of this incident to potentially affected individuals, which includes one (1) New Hampshire resident. 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

The confidentiality, privacy, and security of information is one of Oregon Tech's highest priorities. Upon learning of this incident, Oregon Tech immediately took steps to assess the security of its systems and conduct a thorough investigation. In response to this incident, Oregon Tech is reviewing its security policies and procedures and reassessing its technical, administrative, and physical safeguards to identify and implement further security enhancements, as needed. Oregon Tech is also conducting additional employee training on data privacy and security.

Oregon Tech is providing access to credit monitoring services for one (1) year, through Kroll, to individuals whose personal information was present on the potentially affected systems at the time of the incident. Access to this service will be provided at no cost to these individuals.

Additionally, Oregon Tech is providing affected individuals with guidance on how to 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. Oregon Tech is providing individuals with 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 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. In an abundance of caution, Oregon Tech has notified law enforcement of this incident.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4775.

Very truly yours,

Christopher J. DiIenno of
MULLEN COUGHLIN LLC

CJD/alc
Enclosure

EXHIBIT A

Oregon TECH
Oregon Institute of Technology

<<Date>> (Format: Month Day, Year)

<<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

Re: Notice of Data Breach

Dear <<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>,

Oregon Institute of Technology ("Oregon Tech") wanted to make you aware of a data security incident that may have impacted the security of your personal information. While, to date, Oregon Tech's investigation into this situation has not revealed evidence of actual or attempted misuse of personal information as a result of this incident, we wanted you to be aware of it . Below is background about the incident, our response, and steps you may take to protect against possible misuse of your personal information, should you feel it appropriate to do so.

What happened? On October 25, 2018, Oregon Tech began noticing issues with its network. Oregon Tech immediately began an internal investigation into the activity and discovered that multiple systems were infected with a virus. This investigation included working with third-party forensic investigators to confirm the nature and scope of this incident. On November 16, 2018, the investigation determined that there may have been unauthorized access to certain systems between October 19, 2018 through October 23, 2018. Unfortunately, this investigation was unable to determine what information, if any, was accessed within those systems.

Oregon Tech then initiated another investigation, to review the potentially affected systems to determine if there was any personal information present on those systems at the time of the incident. This review required an extensive systematic and manual review of the files and documents stored on the potentially affected systems. On March 3, 2019, Oregon Tech concluded this review and determined that personal information was present on the relevant systems at the time of the incident. Since that time, Oregon Tech has been diligently reviewing this information and its records for purposes of disclosing this incident to potentially affected individuals. As noted above, to date, Oregon Tech's investigation has not revealed evidence of actual or attempted misuse of personal information as a result of this incident.

What Information was Involved? Our investigation confirmed the potentially affected systems contained information including your <<ClientDef1(name, address[and /,][insert field with specific information])>>. Please note that while our investigation did not reveal evidence that this information was actually viewed by an unauthorized actor, we are providing you this notice to ensure you are aware of this incident.

What We Are Doing. The confidentiality, privacy, and security of information is one of our highest priorities. Upon learning of this incident, we immediately took steps to assess the security of our systems and conduct a thorough investigation. In response to this incident, we are reviewing our security policies and procedures and reassessing our technical, administrative, and physical safeguards to identify and implement further security enhancements, as needed. We are also conducting additional employee training on data privacy and security.

As an added precaution, we are offering you access to one year of credit monitoring and identity theft restoration services through Kroll at no cost to you.

What You Can Do. You may review the enclosed "Steps You Can Take to Protect Your Information," which contains information on what you can do to protect against possible misuse of your information. You may also enroll in the credit monitoring and identity theft restoration services we are offering, as we are unable to do so on your behalf.

For More Information. We understand you may have questions that are not answered in this letter. If you have questions, please contact 1-866-775-4209, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time. Please have your membership number ready.

You may also write to us at 3201 Campus Drive, Klamath Falls, OR 97601.

Thomas Keyser
Dean of College
Oregon Institute of Technology

STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **krollbreach.idMonitoringService.com** to activate and take advantage of your identity monitoring services.

*You have until **July 15, 2019** to activate your identity monitoring services.*

Membership Number: <<Member ID>>

To receive credit services by mail instead of online, please call 1-844-263-8605. Additional information describing your services is included with this letter.

Monitor Your Accounts

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 and to detect errors. 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

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 2002
Allen, TX 75013
1-888-397-3742
www.experian.com/fraud/center.html

TransUnion
P.O. Box 2000
Chester, PA 19106
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

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. Oregon Institute of Technology is located at 3201 Campus Drive, Klamath Falls, OR 97601.

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 violator. 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 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.

Kroll. | A Division of DUFF&PHELPS

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services[1] from Kroll:

Single Bureau Credit Monitoring. You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

Fraud Consultation. You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration. If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

[1] Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.