MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

M. Alexandra Belton
Office: 267-930-4773
Fax: 267-930-4771
Email: abelton@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

June 5, 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 Event

Dear Attorney General MacDonald:

This office represents the University of Alaska System ("UA"), 910 Yukon Drive, Fairbanks, AK 99775. We write to provide you with notice of an incident that may impact the security of personal information relating to fourteen (14) New Hampshire residents. The investigation into this event is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, UA does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

Nature of the Data Event

In February 2018, UA began receiving reports from UAOnline system users of issues accessing their UAOnline accounts. UA immediately took steps to terminate unauthorized access, initiated an investigation, and began working with third-party forensic experts to assist in determining the impact of this activity. Based on the investigation, UA determined that certain users' UAOnline account passwords were changed by an unauthorized third party. In February 2018, UA notified all UAOnline users whose accounts were affected and upgraded security protocols for password changes.

Following the notification to affected UAOnline users, UA continued to investigate the unauthorized access to the UA system to confirm the full nature and scope of the activity. That investigation included a thorough review of other university systems and applications. Through this review, on or around March 28, 2018, the investigation determined that an unauthorized user also may have accessed certain email accounts between January 31, 2018 and February 15, 2018. UA expanded the investigation to include a comprehensive programmatic and manual review of the affected email accounts to determine whether sensitive information was present and to whom such records related. UA then worked diligently to determine the identity and contact information for individuals whose information may have been present in the email accounts at the time of the unauthorized access.

The investigation determined that the information present in the impacted email accounts may include the following data related to certain New Hampshire residents: Social Security Number, financial account number.

Notice to the New Hampshire Residents

On or about June 5, 2019, UA provided written notice of this incident to potentially affected individuals, which includes fourteen (14) New Hampshire residents. This notice was provided in substantially the same form as the communication attached hereto as ***Exhibit A***. In addition to written notice, UA provided notice to potentially affected individuals by issuing a nationwide press release and posted notice of the data event on its website on April 24, 2019. A copy of the press release and web posting is attached hereto as ***Exhibit B*** and ***Exhibit C***, respectively.

Other Steps Taken and To Be Taken

Since receiving reports of issues with UA online systems, UA has worked diligently to investigate and remediate this incident, confirm the security of its systems, and provide the known affected individuals with notice of this event. While UA has security measures in place to safeguard data in its care, it has also taken steps to enhance the security of its password reset manager and implement password changes for those users whose accounts are known to be affected.

UA is also providing written notice to those individuals whose data may have been present in the accounts impacted by this incident. This notice will include an offer of access to one (1) year of complimentary credit and identity monitoring services, including identity restoration services, through TransUnion, and the contact information for a dedicated call center for potentially affected individuals to contact with questions or concerns regarding this incident. Additionally, UA 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 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. UA has also reported this incident to the U.S. Department of Education, as well as other applicable state regulators.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at 267-930-4773.

Very truly yours,

M. Alexandra Belton of
MULLEN COUGHLIN LLC

MAB/crm
Enclosure

EXHIBIT A

University Of Alaska Incident - 6537
PO Box 44
Minneapolis, MN 55440-0044

UNIVERSITY of ALASKA
Many Traditions One Alaska

* C L M N T I D N O * - UAA - <<SequenceNo>>

<<Name1>>
<<Name2>>
<<Name3>>
<<Name4>>
<<Address1>>
<<Address2>>
<<City>> <<State>> <<Zip10>>
<<CountryName>>

<<Date>>

RE: Notice of Data Breach

Dear <<Name1>>,

We write to inform you of a recent event that may affect the privacy of some of your personal information. The University of Alaska ("UA") takes this incident very seriously and is providing you with information and access to resources so that you may better protect your personal information, should you feel it is appropriate to do so.

What Happened? In February 2018, UA began receiving reports from UAOnline system users of issues accessing their UAOnline accounts. UA immediately took steps to terminate unauthorized access, initiated an investigation, and began working with third-party forensic experts to assist in determining the impact of this activity. Based on the investigation, UA determined that certain users' UAOnline account passwords were changed by an unauthorized third party. In February 2018, UA notified all UAOnline users whose accounts were affected and upgraded security protocols for password changes.

Following the notification to affected UAOnline users, UA continued to investigate the unauthorized access to the UA system to confirm the full nature and scope of the activity. That investigation included a thorough review of other university systems and applications. Through this review, on or around March 28, 2018, the investigation determined that an unauthorized user also may have accessed certain email accounts between January 31, 2018 and February 15, 2018. UA expanded the investigation to include a comprehensive programmatic and manual review of the affected email accounts to determine whether sensitive information was present and to whom such records related. UA then worked diligently to determine the identity and contact information for individuals whose information may have been present in the email accounts at the time of the unauthorized access. Through this review, we determined your information was present in an impacted email account.

What Information Was Involved? Our investigation determined that the information related to you that was present in the emails included: <<data elements>>.

What We Are Doing. Upon learning of potential unauthorized access to certain email accounts, UA immediately took steps to respond and worked with outside experts to confirm the nature and scope of the incident and identify any individuals whose information may have been present in the emails potentially subject to unauthorized access. UA is notifying you of this incident and providing you with information you may use to better protect against potential misuse of personal information, should you feel it appropriate to do so. While UA has security measures in place to protect information in its care, we are also taking steps to evaluate additional safeguards and review policies and procedures in order to protect the security of its data.

As an added precaution, we are also offering you access to 12 months of credit monitoring and identity theft restoration services through TransUnion at no cost to you. The cost of this service will be paid for by the University of Alaska. We encourage you to enroll in these services, as we are not able to act on your behalf to enroll you in the credit monitoring service.

What You Can Do. Please review the enclosed "Steps You Can Take to Protect Personal Information." You can also enroll to receive the free credit monitoring and identity theft protection services we are offering.

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 (866) 783-5580 between 5 AM and 6 PM PST Monday through Friday excluding major U.S. holidays.

Again, UA takes the privacy and security of the personal information in our care earnestly. We sincerely regret any concern or inconvenience this incident may cause you.

Sincerely,

Mark Kondrak
Chief Information Technology Officer

Steps You Can Take to Protect Personal Information

Enroll in the Credit Monitoring

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

To enroll in this service, go to the *my*TrueIdentity website at **www.mytrueidentity.com** and in the space referenced as "Enter Activation Code", enter the following 12-letter Activation Code **<<ActivationCode>>** 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 following 6-digit telephone pass code **<<PassCode>>** 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 **August 31, 2019**. 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.

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, change of address and more. The service also includes the ability to lock and unlock your credit report, access to an identity restoration program that provides assistance in the event 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.)

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 accounts and 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	**TransUnion**	**Equifax**
PO Box 9554	P.O. Box 2000	PO Box 105788
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	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	**TransUnion**	**Equifax**
P.O. Box 2002	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	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 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 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 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 are XXX Rhode Island residents potentially impacted by this incident.

EXHIBIT B

UNIVERSITY OF ALASKA MEDIA CONTACT:	For Immediate Release:
Alexandra Belton 267-930-4773 abelton@mullen.law	Fairbanks, Alaska [Date]

UNIVERSITY OF ALASKA - NOTICE OF DATA BREACH

The University of Alaska is notifying affected students and individuals after an investigation into a data privacy incident involving potential unauthorized access to certain UA email accounts. University of Alaska is notifying individuals whose records were or may have been in the email accounts at the time of the unauthorized access and is providing these individuals with information and resources that can be used to better protect against the possible misuse of information.

What Happened? In February 2018, University of Alaska (UA) began receiving reports from UAOnline system users of issues accessing their UAOnline accounts. UA immediately took steps to terminate unauthorized access, initiated an investigation, and began working with third-party forensic experts to assist in determining the impact of this activity. Based on the investigation, UA determined that certain users' UAOnline account passwords were changed by an unauthorized third party. In February 2018, UA notified all UAOnline users whose accounts were affected and upgraded security protocols for password changes.

Following the notification to affected UAOnline users, UA continued to investigate the unauthorized access to the UA system to confirm the full nature and scope of the activity. That investigation included a thorough review of other university systems and applications. Through this review, on or around March 28, 2018, the investigation determined that an unauthorized user also may have accessed certain email accounts between January 31, 2018 and February 15, 2018. UA expanded the investigation to include a comprehensive programmatic and manual review of the affected email accounts to determine whether protected information was present and to whom such records related. UA then worked diligently to determine the identity and contact information for individuals whose information may have been present in the email accounts at the time of the unauthorized access. This process was completed on or around February 25, 2019.

What Information Was Involved? The information that may have been present in the affected email accounts varies by individual; however, it may include an individual's name, government issued identification number, date of birth, digital signature, driver's license number, usernames and/or passwords, financial account numbers, health and/or health insurance information, passport number, and UA student identification number. For certain individuals, Social Security number may also have been present in the affected email accounts.

What UA Is Doing. Upon learning of potential unauthorized access to certain email accounts, UA immediately took steps to respond and worked with outside experts to confirm the nature and scope of the email incident and identify any individuals whose information may have been present in the emails potentially subject to unauthorized access. UA is notifying potentially affected individuals of this incident, providing them with access to credit monitoring, and providing information and access to resources they may use to better protect against potential misuse of personal information, should they feel it appropriate to do so. While UA has security measures in place to protect information in its care, it is also taking steps to evaluate additional safeguards and review policies and procedures in order to protect the security of information on our systems.

What You Can Do. UA encourages potentially affected individuals to review the information it is providing on "Steps Individuals Can Take To Protect Information."

For More Information. To assist individuals who may have further questions about this incident, UA has established a toll-free hotline. This dedicated assistance line may be reached by calling [XXX-XXX-XXXX], Monday through [XXXX], [X] a.m. to [X] p.m. PST (excluding US holidays). Additional information may also be

found at https://www.alaska.edu/news/it/dataincident.php. The University will not contact you by phone to request any personal information.

STEPS INDIVIDUALS CAN TAKE TO PROTECT INFORMATION

UA encourages potentially impacted individuals to remain vigilant against incidents of identity theft and fraud, to review account statements, and to monitor credit reports for suspicious activity. Under U.S. law adults over the age of 18 are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order a 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.

Individuals with credit files have the right to place a "security freeze" on their credit report, which will prohibit a consumer reporting agency from releasing information in the credit report without the individual's express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in an individual's name without his or her consent. However, be aware that using a security freeze to take control over who gets access to the personal and financial information in a credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application made 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, individuals with credit files have the right to place an initial or extended "fraud alert" on their files at no cost. An initial fraud alert is a 1-year alert that is placed on an individual's credit file. Upon seeing a fraud alert display on an individual's credit file, a business is required to take steps to verify the individual'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-

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

victim-resource/place-fraud-alert report-services

Further information regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, is available 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. UA's main campus is located at 2025 Yukon Drive, Fairbanks, AK 99775.

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 Rhode Island Residents: The Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, 1-401-247-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are XXX Rhode Island residents impacted by this incident.

For Massachusetts Residents: You have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

EXHIBIT C

NOTICE OF DATA BREACH

ABOUT THE DATA PRIVACY INCIDENT

The University of Alaska ("UA") is notifying potentially affected students and individuals after an investigation into a data privacy incident involving unauthorized access to certain UA email accounts. UA is notifying individuals whose records were or may have been in the email accounts at the time of the unauthorized access and is providing these individuals with information and resources that can be used to better protect against the possible misuse of information.

What Happened? In February 2018, University of Alaska (UA) began receiving reports from UAOnline system users of issues accessing their UAOnline accounts. UA immediately took steps to terminate unauthorized access, initiated an investigation, and began working with third-party forensic experts to assist in determining the impact of this activity. Based on the investigation, UA determined that certain users' UAOnline account passwords were changed by an unauthorized third party. In February 2018, UA notified all UAOnline users whose accounts were affected and upgraded security protocols for password changes.

Following the notification to affected UAOnline users, UA continued to investigate the unauthorized access to the UA system to confirm the full nature and scope of the activity. That investigation included a thorough review of other university systems and applications. Through this review, on or around March 28, 2018, the investigation determined that an unauthorized user also may have accessed certain email accounts between January 31, 2018 and February 15, 2018. UA expanded the investigation to include a comprehensive programmatic and manual review of the affected email accounts to determine whether protected information was present and to whom such records related. UA then worked diligently to determine the identity and contact information for individuals whose information may have been present in the email accounts at the time of the unauthorized access. This process was completed on or around February 25, 2019.

What Information Was Involved? The information that may have been present in the affected email accounts varies by individual; however, it may include an individual's name, government issued identification number, date of birth, digital signature, driver's license number, usernames and/or passwords, financial account numbers, health and/or health insurance information, passport number, and UA student identification number. For certain individuals, Social Security number may also have been present in the affected email accounts.

What UA Is Doing. Upon learning of potential unauthorized access to certain email accounts, UA immediately took steps to respond and worked with outside experts to confirm the nature and scope of the email incident and identify any individuals whose information may have been present in the emails potentially subject to unauthorized access. UA is notifying potentially affected individuals of this incident, providing them with access to credit monitoring, and providing information and access to resources they may use to better protect against potential misuse of personal information, should they feel it appropriate to do so. While UA has security measures in place to protect information in its care, it is also taking steps to evaluate additional safeguards and review policies and procedures in order to protect the security of information on our systems.

What You Can Do. UA encourages potentially impacted individuals to remain vigilant against incidents of identity theft and fraud, to review account statements, and to monitor credit reports for suspicious activity.

Under U.S. law adults over the age of 18 are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order a 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.

Individuals with credit files have the right to place a "security freeze" on their credit report, which will prohibit a consumer reporting agency from releasing information in the credit report without the individual's express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in an individual's name without his or her consent. However, be aware that using a security freeze to take control over who gets access to the personal and financial information in a credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application made 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	**TransUnion**	**Equifax**
PO Box 9554	P.O. Box 2000	PO Box 105788
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	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.

The credit reporting agencies have one (1) to three (3) business days after receiving your request to place a security freeze on your credit file report, based upon the method of the request. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with the process by which you may remove the security freeze, including an authentication mechanism. Upon receiving a direct request from you to remove a security freeze and upon receiving proper identification from you, the consumer reporting agency shall remove a security freeze within one (1) hour after receiving the request by telephone for removal or within three (3) business days after receiving the request by mail for removal.

As an alternative to a security freeze, individuals with credit files have the right to place an initial or extended "fraud alert" on their files at no cost. An initial fraud alert is a 1-year alert that is placed on an individual's credit file. Upon seeing a fraud alert display on an individual's credit file, a business is required to take steps to verify the individual'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	**TransUnion**	**Equifax**
P.O. Box 2002	P.O. Box 2000	P.O. Box 105069

Allen, TX 75013 1-888-397-3742 www.experian.com/fraud/center.html	Chester, PA 19106 1-800-680-7289 www.transunion.com/fraud-victim-resource/place-fraud-alert	Atlanta, GA 30348 1-888-766-0008 www.equifax.com/personal/credit-report-services

Further information regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, is available 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. UA's main campus is located at 2025 Yukon Drive, Fairbanks, AK 99775.

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 Rhode Island Residents: The Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, 1-401-247-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are XXX Rhode Island residents impacted by this incident.

For Massachusetts residents, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For More Information. To assist individuals who may have further questions about this incident, UA has established a toll-free hotline. This dedicated assistance line may be reached by calling [XXX-XXX-

XXXX], Monday through [XXXX], [X] a.m. to [X] p.m. PST (excluding US holidays). The University will not contact you by phone to request any personal information.