



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Gregory J. Bautista
Office: (267) 930-1509
Fax: (267) 930-4771
Email: gbautista@mullen.law

1266 E. Main Street, Soundview Plaza,
Suite 700 R
Stamford, CT 06902

April 5, 2023

VIA E-MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Notice of Data Event

To Whom It May Concern:

We represent Northern Arizona University (“NAU”) located at 1900 S Knoles Drive, Flagstaff, AZ 86011, and are writing to notify your office of an incident that may affect the security of certain personal information relating to one (1) Maryland resident. This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, NAU does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about February 7, 2022, NAU discovered suspicious activity involving certain employee email accounts and initiated an investigation. As part of the investigation, which was conducted by third-party forensic specialists, it was determined that certain employee email accounts were accessed without authorization between February 7, 2022 to February 8, 2022. The investigation could not confirm what specific information within these accounts may have been accessed by the unauthorized individual. Therefore, in an abundance of caution, NAU then undertook a diligent and comprehensive review of the entire contents of the impacted email accounts to determine the full universe of information present in these accounts and potentially subject to unauthorized access. On or around March 6, 2023, the full scope of this comprehensive review was completed, and NAU confirmed whose information was potentially accessed.

The information that could have been subject to unauthorized access includes name, address, financial account information, health insurance information, and medical information.

Notice to Maryland Resident

On or about April 5, 2023, NAU provided written notice of this incident to one (1) Maryland 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

Upon discovering the event, NAU moved quickly to investigate and respond to the incident, assess the security of NAU systems, and identify potentially affected individuals. NAU is also working to implement additional safeguards and training to its employees. NAU is providing access to credit monitoring services for twelve (12) months, through Experian, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, NAU 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. NAU 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.

NAU is providing written notice of this incident to relevant state and federal regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-1509.

Very truly yours,



Gregory J. Bautista of
MULLEN COUGHLIN LLC

GJB /kzf
Enclosure

EXHIBIT A



Return Mail Processing
PO Box 999
Suwanee, GA 30024

8 1 1157 *****SNGLP

SAMPLE A. SAMPLE - L01

APT ABC



123 ANY ST

ANYTOWN, US 12345-6789



April 5, 2023

NOTICE OF [Extra1]

Dear Sample A. Sample:

Northern Arizona University (“NAU”) is writing to notify you of a data security event that may affect the privacy of some of your information. Although NAU is currently unaware of any misuse of your information, we are nonetheless providing you with details about the incident, NAU’s response, and steps you may take to protect against misuse of your information, should you feel it necessary to do so.

What Happened? On or about February 7, 2022, NAU discovered suspicious activity involving certain employee email accounts and initiated an investigation. As part of the investigation, which was conducted by third-party forensic specialists, it was determined that certain employee email accounts were accessed without authorization between February 7, 2022 to February 8, 2022. The investigation could not confirm what specific information within these accounts may have been accessed by the unauthorized individual. Therefore, in an abundance of caution, NAU then undertook a diligent and comprehensive review of the entire contents of the impacted email accounts to determine the full universe of information present in these accounts and potentially subject to unauthorized access. On or around March 6, 2023, the full scope of this comprehensive review was completed, and NAU confirmed that certain information related to you was present in the relevant accounts at the time of the incident, and thus potentially accessible.

What Information Was Involved? The information related to you that may be affected includes: [Extra2] and name. Please note that while our investigation has not identified any actual or attempted misuse of your information, we are providing you this notice to ensure you are aware of this incident.

What We Are Doing. Data privacy and security are among NAU’s highest priorities, and there are extensive measures in place to protect information in NAU’s care. Upon discovery, NAU promptly commenced an investigation with the assistance of third-party cyber security specialists to confirm the nature and scope of this incident. NAU is providing notice of this incident to impacted individuals and pertinent state and/or federal regulators. As part of NAU’s ongoing commitment to the security of information, all policies and procedures are being reviewed and enhanced where possible, additional safeguards are being implemented, and workforce training is being conducted to reduce the likelihood of a similar event in the future.

As an added precaution, we are also offering [Extra3] of complimentary access to credit monitoring services through Experian. If you wish to activate the credit monitoring services, you may follow the instructions included in the *Steps You Can Take to Help Protect Personal Information*.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, explanation of benefits, and credit reports for suspicious activity. You may also review the information contained in the attached *Steps You Can Take to Help Protect Personal Information*. We encourage you to enroll to receive the complimentary credit monitoring services being provided by NAU. NAU will cover the cost of these services; however, you will need to enroll yourself as we are unable to do so on your behalf.

For More Information. We understand you may have questions that are not addressed in this letter. If you have additional questions, or need assistance, please call our toll-free number at (833) 549-0267, Monday - Friday from 7 am to 9 pm MT, or Saturday - Sunday from 9 am to 6 pm MT (Excluding major U.S. holidays). Please be prepared to provide engagement number [Engagement Number]. You may also write to NAU at 1900 S Knoles Drive, Flagstaff, AZ 86011.

We apologize for any inconvenience this incident may have caused you.

Sincerely,

Information Security Services

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

Enroll in Credit Monitoring

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for [Extra3] months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for [Extra3] months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary [Extra3]-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll** by June 30, 2023 (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code**: ABCDEFGHI

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at (833) 549-0267 by June 30, 2023. Be prepared to provide engagement number [Engagement Number] as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR [EXTRA3]-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARETM:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance^{**}:** Provides coverage for certain costs and unauthorized electronic fund transfers.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and Transunion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit 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 three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit 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 credit 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 credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to 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, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	Transunion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.Transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	Transunion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	Transunion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and 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 District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and 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 bureaus 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 North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

