



MULLEN
COUGHLIN_{LLC}
ATTORNEYS AT LAW

Carolyn Purwin Ryan
Office: (267) 930-6836
Fax: (267) 930-4771
Email: CPurwinRyan@mullen.law

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

January 9, 2024

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 The Chronicle of Higher Education (“The Chronicle” or “Chronicle”), located at 1255 23rd Street, N.W., Suite 700, Washington, DC 20037, and are writing to notify your office of an event that may affect the security of certain personal information relating to approximately one (1) Maryland resident. This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, The Chronicle 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 July 25, 2023, The Chronicle became aware of suspicious activity in its email environment. The Chronicle immediately launched an investigation, with the assistance of third-party cybersecurity specialists, to determine the nature and scope of the event. The investigation determined that between January 12, 2023 and July 25, 2023, an unauthorized actor gained access to certain Chronicle email accounts and may have viewed certain information contained therein.

The Chronicle conducted a thorough and comprehensive review to identify individuals whose personal information was potentially accessed during the event. Once complete, The Chronicle also worked to validate the results of the review and identify appropriate contact information for those potentially affected. The Chronicle completed this process on December 22, 2023, and then moved as quickly as possible to provide notice. The personal information related to Maryland

residents that could have been subject to unauthorized access includes the following: name, address, and Social Security number.

Notice to Maryland Resident

On January 9, 2024, The Chronicle provided written notice of this event to potentially impacted individuals, including approximately 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 becoming aware of the event, The Chronicle moved quickly to investigate and respond to the event, assess the security of The Chronicle's systems and email environment, and identify potentially affected individuals. The Chronicle is working to implement additional safeguards and training to its employees. The Chronicle also is providing access to credit monitoring and identity restoration services for twelve (12) months, through Experian, to Maryland residents whose personal information was potentially affected by this incident, at no cost to the individuals.

Additionally, The Chronicle 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 bank or financial institution. The Chronicle is providing individuals with information on how to place a fraud alert and credit 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. The Chronicle is also providing written notice of this incident to relevant state regulators, as required.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-6836.

Very truly yours,

Carolyn Purwin Ryan of
MULLEN COUGHLIN LLC

CPR/aml
Enclosure

EXHIBIT A

THE CHRONICLE OF HIGHER EDUCATION

The Chronicle of Higher Education, Inc.
1255 23rd Street, N.W., Suite 700
Washington, DC 20037

<<First Name>> <<MI>> <<Last Name>> <<Suffix>>

<<Address 1>>

<<Address 2>>

<<Date>>

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

<<Country>>

<<VARIABLE HEADER FIELD>>

Dear <<First Name>> <<MI>> <<Last Name>> <<Suffix>>:

The Chronicle of Higher Education (“The Chronicle” or “Chronicle”) is writing to inform you of an event that may impact the security of some of your information. Although we have received no indication of any actual or attempted identity theft or fraud of your information as a result of this event, this notice provides information about the event, our response, and resources available to you to help protect your information from possible misuse, should you feel it is necessary to do so.

What Happened? On July 25, 2023, The Chronicle became aware of suspicious activity in its email environment. We immediately launched an investigation, with the assistance of third-party cybersecurity specialists, to determine the nature and scope of the event. The investigation determined that between January 12, 2023 and July 25, 2023, an unauthorized actor gained access to certain Chronicle email accounts and may have viewed certain information contained therein. Therefore, we conducted a thorough and comprehensive review to identify individuals whose personal information was potentially accessed during the event. Once complete, we also worked to validate the results of the review and identify appropriate contact information for potentially affected individuals. We completed this process on December 22, 2023, and then moved as quickly as possible to provide notice.

What Information Was Involved? There is no evidence that information was actually accessed, viewed, or acquired as a result of this event. Nonetheless, the investigation determined that your name, address, <<Variable Text 1>>, were potentially accessible.

What We Are Doing. The confidentiality, privacy, and security of information in our care are among our highest priorities. Upon becoming aware of the event, we moved quickly to investigate and respond to the event, assess the security of our network and email environment, and notify potentially affected individuals. We are notifying potentially affected individuals, including you, so that you may take further steps to best protect your information, should you feel it is necessary to do so. We regret any inconvenience or concern this event may cause. As an added precaution, we are offering credit monitoring and identity restoration services through Experian for twelve (12) months, at no cost to you.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and credit reports for suspicious activity and to report any suspicious activity promptly to your bank or financial institution. Additional information and resources are included in the enclosed *Steps You Can Take To Protect Personal Information*. You may also enroll in the complimentary credit monitoring and identity restoration services available to you. Enrollment instructions are attached to this letter.

For More Information. We understand that you may have questions about this event that are not addressed in this letter. If you have additional questions, please call the dedicated assistance line at (202) 466-1236, Monday through Friday from 9:00 a.m. to 5:00 p.m. Eastern Time, excluding major U.S. holidays. Please have this letter ready if you call. Again, we

take the privacy and security of information in our care very seriously and sincerely regret any inconvenience or concern this event may cause you.

Sincerely,

Maureen Ryan
Associate Director
The Chronicle of Higher Education

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Monitoring Services

To help protect your identity, we are offering a complimentary 12-month membership of Experian's® IdentityWorksSM. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by: April 30, 2024** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code: <<Code>>**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-890-9332 by **April 30, 2024**. Be prepared to provide engagement number **B112833** as proof of eligibility for the identity restoration services by Experian.

Additional details regarding your 12-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.¹
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents 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.
- **Up to \$1 Million Identity Theft Insurance²:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 877-890-9332. 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 (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 this Identity Restoration support is available to you for twelve (12) 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. You will also find self-help tips and information about identity protection at this site.

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 a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

¹ Offline members will be eligible to call for additional reports quarterly after enrolling.

² 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.

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 consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any 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 a consumer’s name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of 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 they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, 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

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 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. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

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 <https://www.marylandattorneygeneral.gov/>.