



MULLEN
COUGHLIN_{LLC}
ATTORNEYS AT LAW

Ryan C. Loughlin
Office: (267) 930-4786
Fax: (267) 930-4771
Email: rloughlin@mullen.law

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

March 22, 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: Courtesy Notice of Data Event

To Whom It May Concern:

We represent Colorado Department of Higher Education (“CDHE”) located at 1600 Broadway, Suite 2200, Denver, CO 80202, and write 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, CDHE 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 June 19, 2023, CDHE became aware it was the victim of a cybersecurity ransomware incident that impacted its network systems. CDHE took steps to secure the network and has been working with third-party specialists to conduct a thorough investigation into this incident. CDHE also worked to restore systems and return to normal operations.

While this incident is still part of an ongoing criminal and internal investigation, CDHE knows that an unauthorized actor(s) accessed CDHE systems between June 11 and June 19, 2023 and that certain data was copied from CDHE systems during this time. As part of its ongoing investigation, CDHE conducted a thorough review of the data in order to determine what specific information was present in the files and to whom it relates. Through the data review and validation process, CDHE identified additional individuals who may be impacted by this incident.

Notice to Maryland Resident

On August 4, 2023, after preliminary investigation, CDHE began providing notice to potentially impacted individuals via its website, to Colorado media and via mail and email where CDHE had mailing address and emails. The review of the impacted records was ongoing and once complete, CDHE notified potentially impacted individuals by mail or email for individuals for whom CDHE have contact information.

On or about February 15, 2024, upon completion of data review and validation process, CDHE provided updated notice accounting for this additional population via its website and to the media. On or about March 21, 2024, CDHE also provided written notice to potentially impacted individuals including one (1) Maryland resident for whom it had contact information. The impacted information varies by individual but personal information includes name and Social Security number.

A copy of the written notice is attached here as *Exhibit A*.

Other Steps Taken and To Be Taken

In response to this incident, CDHE is reviewing its policies and procedures and working to implement additional cybersecurity safeguards to further protect its systems. Additionally, CDHE is providing impacted individuals with complimentary access to two (2) years of credit monitoring and identity theft protection services through Experian. Additionally, CDHE is providing impacted individuals with guidance on how to better protect against identity theft and fraud. CDHE 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.

CDHE provided written notice of this incident to relevant 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) 930-4786.

Very truly yours,



Ryan C. Loughlin of
MULLEN COUGHLIN LLC

RCL/ajl
Enclosure

EXHIBIT A



COLORADO
Department of
Higher Education

1600 Broadway, Suite 2200
Denver, CO 80202

Jared Polis
Governor

Dr. Angie Paccione
Executive Director

<<Name 1>> <<Name 2>>
<<Address 1>>
<<Address 2>>
 <<Date>>
<<City>>, <<State>> <<Zip>>
<<Country>>

Re: Updated Notice

Dear <<Name 1>> <<Name 2>>:

We write to inform you of a cybersecurity incident involving the Colorado Department of Higher Education (“CDHE”) that may involve your personal information. As you may know, CDHE receives information from colleges, universities, the Colorado Department of Education, and other sources to deliver services to residents of Colorado. Pursuant to Colorado State law, we are providing you with this notification so that you may take action to protect yourself against identity theft or other possible misuse of your information.

What Happened?

On June 19, 2023, CDHE became aware it was the victim of a cybersecurity ransomware incident that impacted its network systems. CDHE took steps to secure the network and has been working with third-party specialists to conduct a thorough investigation into this incident. CDHE has also worked to restore its systems and return to normal operations.

While this incident is still part of an ongoing criminal and internal investigation, CDHE knows that an unauthorized actor(s) accessed CDHE systems between June 11 and June 19, 2023, and that certain data was copied from CDHE systems during this time. Based on preliminary review, CDHE provided notice of this incident on its website and through the media on August 4, 2023. As part of its ongoing investigation, CDHE conducted a thorough review of the data to determine what specific information was present in the files and to whom it relates. Through the data review and validation process, we recently identified some personal information relating to you.

What Information Was Involved?

Your [Data Elements] were present in the impacted files.

What We Are Doing

In response to this incident, CDHE is reviewing its policies and procedures and is working to implement additional cybersecurity safeguards to further protect its systems. In addition, CDHE



is offering you two years of free credit monitoring and identity theft protection services through Experian. Unfortunately, CDHE cannot enroll you directly. If you would like to enroll, please review the information contained in the attached [Steps You Can Take to Help Protect Personal Information](#).

What You Can Do

Actions you can take to prevent identity theft and fraud include reviewing your account statements and monitoring your free credit reports for suspicious activity and detecting errors. We also encourage you to enroll in the monitoring services provided to you.

For More Information

We understand that you may have additional questions. For assistance with questions regarding this incident, please call our designated hotline at (833) 301-1346 between 7 a.m. to 9 p.m. Mountain Time, Monday through Friday (excluding U.S. holidays), 9 a.m. to 6 p.m. Mountain Time, Saturday and Sunday (excluding U.S. holidays). You may also visit <https://cdhe.colorado.gov/> for more information.

Sincerely,



Dr. Angie Paccione, Executive Director
Colorado Department of Higher Education



STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

Enroll in Monitoring Services

To help protect your identity, CDHE is offering complimentary access to Experian IdentityWorksSM for 24 months.

Please note that Identity Restoration is available to you for 24 months from the date of this notice. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to individuals, we also encourage to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 24-month membership. This product provides individuals with superior identity detection and resolution of identity theft. To start monitoring personal information, please follow the steps below:

- Ensure that you **enroll by May 31, 2024** (Code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll:
<https://www.experianidworks.com/credit>
- Provide your **activation code: [Activation Code]**

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. 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).

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 (833) 301-1346 by May 31, 2024. Please be prepared to provide engagement number **B116620** as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING 24-MONTH EXPERIAN IDENTITYWORKSSM 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

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



- 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 ExtendCARE™: 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.

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.

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.

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.



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; 1-410-576-6300 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.

