Figure 1

FREQUENTLY ASKED QUESTIONS

1. **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 is working with third-party specialists to conduct a thorough investigation into this incident.

While this incident is still part of an ongoing criminal investigation, our internal investigation has indicated that an unauthorized actor(s) accessed CDHE systems on June 19, 2023, and that certain data was copied from CDHE systems during this time. Over the past few weeks, our ongoing investigation has revealed that some of the records may include name and social security number or student identification number, as well as other education records.

The Colorado Department of Higher Education is providing an update to its August 4, 2023, notice of a cybersecurity incident that involved the personal information of certain individuals. Since the prior notice, CDHE contracted with a third-party vendor to conduct a thorough data review and determined that those who enrolled in a **Federal TRIO program in Colorado before 2017, those who attended a public high school in Colorado between school years 2020-2021 or 2021-2022, or those who took a GED exam in Colorado prior to 2012** may be impacted by this incident. These individuals are encouraged to enroll in credit monitoring services.

2. **Who is impacted?**

Those who attended a public institution of higher education in Colorado between 2007-2020, enrolled in a Federal TRIO program in Colorado prior to 2017, attended a Colorado public high school between 2004-2022, individuals with a

Colorado K-12 public school educator license between 2010-2014, participated in the Dependent Tuition Assistance Program from 2009-2013, participated in Colorado Department of Education's Adult Education Initiatives programs between 2013-2017, or took a GED exam in Colorado prior to 2012 were impacted by this incident.

In addition, specific individuals not on the above list may be impacted if they received a letter indicating that they were impacted. Those include:

- A small group of students who attended Mile High Medical Academy
- Students who were reverse transfer students in 2012
- A small group of current and former CDHE staff

Individuals in these three groups who did not receive an individual notification are not impacted.

3. **Why does CDHE have my information?**

CDHE collects student information from various institutions in Colorado and works closely with other state agencies.

4. **I have not been a student for years. Why do you still have my information?**

CDHE maintains student records consistent with its requirements under federal and state law and internal policies and regulations.

5. **When did CDHE become aware of this?**

On June 19, 2023, CDHE became aware it was the victim of a cybersecurity ransomware incident that impacted its network systems.

6. **Why did it take from June until now to send notifications?**

Since first learning of the incident, CDHE has diligently been working to gather information about the incident from its investigation and determining what information may have been affected. Based on such efforts, CDHE provided notice, via email, letter, and its website, as soon as it was reasonably able to do so. As part of its 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 and provided notice.

7. **What information was potentially accessed/affected?**

The specific types of information that may have been affected include name; Social Security number and/or student identification number, and other education records.

8. **How many individuals are impacted?**

We are unable to share that information.

9. **How does one request that information be removed from your system?**

Please request this through an email to CDHE@dhe.state.co.us. Please note that, as a state entity, CDHE must comply with federal, state, local government, and contract records retention regulations.

10. **What is CDHE doing to prevent this from happening again?**

In response to this incident, we are reviewing our policies and procedures and are working to implement additional cybersecurity safeguards to minimize the likelihood of this type of event occurring again. CDHE has already taken several steps to implement additional security safeguards and will continue to do so.

11. **Has this been reported to law enforcement/authorities?**

Yes, CDHE has reported this incident to relevant state and federal regulatory authorities and law enforcement.

12. **If I think I may be the victim of identity theft. What should I do?**

Steps an individual can take to protect against identity theft and fraud include:

Monitoring your financial statements carefully.
If you see any unauthorized or suspicious activity, promptly contact your bank, credit union, or credit card company.

Monitoring your credit reports for suspicious or unauthorized activity.
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.

Placing a fraud alert on your credit file.
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. Contact the three major credit bureaus directly to place a fraud alert on your credit file.

Placing a security freeze on your credit file.
A security freeze 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. Contact the three major credit bureaus directly to place a security freeze on your credit file.

Contacting the Federal Trade Commission and your state Attorney General to learn more about identity theft, fraud alerts, security freezes, and other steps you can take to protect yourself.
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.

Reporting incidents of suspected or actual identity theft or fraud to law enforcement, the Federal Trade Commission, and your state Attorney General.

13. Does this mean my identity has been stolen?

To date, CDHE has no evidence to suggest that impacted information has been used for identity theft or fraud. However, in an abundance of caution, the public notices includes information on free steps you can take to protect your information against that type of activity.

14. Should I report this to law enforcement?

If you believe you are or may be the victim of identity theft or fraud, we encourage you to file a report with law enforcement.

15. How do I get credit monitoring?

If you have questions about whether you are impacted, please call the call center at 833-918-1247 between 7 a.m. to 7 p.m. Mountain Time, Monday through Friday (excluding U.S. holidays). Additional information can also be found at https://cdhe.colorado.gov/notice-of-data-incident.

CDHE is offering complimentary access to Experian IdentityWorks^{SM} for 24 months.

Please note that Identity Restoration is available to potentially impacted individuals for 24 months from the date of this notice. The Terms and Conditions for this offer are located at https://www.experianidworks.com/restoration(opens in new window).

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**: **5ZZ88BB6T**

More information is available at https://cdhe.colorado.gov/notice-of-data-incident.

16. Is this a scam?

This is not a scam. CDHE set up a call center to support its customers and answer questions about the incident in a timely manner. If you would like to validate this incident, you may do so on CDHE's website at https://cdhe.colorado.gov/notice-of-data-incident.