28579

University of Colorado
Boulder | Colorado Springs | Denver | Anschutz Medical Campus

<<Date>> (Format: Month Day, Year)

LEGAL NOTICE OF DATA SECURITY INCIDENT

Dear <<first_name>> <<last_name>>:

I am writing to inform you of a data exposure that may have resulted in your personal information being available to unauthorized individuals. A server that was used by the University of Colorado Boulder (CU) to store graduate program applicant information for the department of Civil, Environmental, and Architectural Engineering within the College of Engineering and Applied Science was inadvertently exposed via the internet, making it available to internet searches. CU immediately removed the server and has conducted a thorough investigation of this incident. Following a rigorous review spanning several weeks, we want to alert you that your personal information was potentially exposed. The information contained in the graduate application you submitted includes your Name, Email Address, Mailing Address, Phone Number, Applicant ID Number, Date of Birth, Ethnicity, and Full Transcripts provided by previous educational institutions, which included your Social Security Number as a personal identifier, in addition to the aforementioned fields.

We have arranged for you to activate, at no cost to you, an online identity monitoring service for 24 months provided by Kroll. Additional information regarding how to activate the complimentary identity monitoring service is enclosed. We encourage you to activate this free service as soon as possible. We have also provided additional information about steps you can take to help protect yourself against fraud and identity theft.

CU created a website to provide up-to-date information regarding this incident. Should you have additional questions or concerns regarding this matter, please do not hesitate to contact us at 303-735-4357 or oithelp@colorado.edu, 7:30a.m. – 7:00 p.m. Mountain Time, Monday – Friday, excluding US holidays.

I want to personally express my deepest regret for any worry or inconvenience that this incident may cause you. I encourage you to activate the complimentary identity monitoring services available to you to further track activity associated with your personal identity.

Sincerely,

Marin Stanek Ph.D.

Vice Chancellor for IT and CIO
University of Colorado Boulder

COMPLIMENTARY IDENTITY MONITORING SERVICES

Kroll provides you with the following features:

Single Bureau Credit Monitoring. You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you'll receive an alert.

Quick Cash Scan monitors short-term and cash-advance loan sources. You'll receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

$1 Million Identity Fraud Loss Reimbursement. Reimburses you for out-of-pocket expenses totaling up to $1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Fraud Consultation. You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration. If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

How to Activate:

1. You must activate your identity monitoring services by February 7, 2023. Your Activation Code will not work after this date.

2. Visit Enroll.krollmonitoring.com/redeem to activate your identity monitoring services.

3. Provide Your Activation Code: <<Monitoring Code>> and Your Verification ID: SF-008566

Due to privacy laws, we cannot activate these services for you directly. Activating these services will not affect your credit score.

ADDITIONAL ACTIONS TO HELP PROTECT YOUR INFORMATION

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/ account statements 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, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

You have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert, 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 lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

As an alternative to a fraud alert, you 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 your 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 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 credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth;
4. Address for the prior two to five years;
5. Proof of current address, such as a current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver's license or identification card); 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 fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

TransUnion	**Experian**	**Equifax**
1-800-680-7289	1-888-397-3742	1-888-298-0045
www.transunion.com	www.experian.com	www.equifax.com
TransUnion Fraud Alert	**Experian Fraud Alert**	**Equifax Fraud Alert**
P.O. Box 2000	P.O. Box 9554	P.O. Box 105069
Chester, PA 19016-2000	Allen, TX 75013	Atlanta, GA 30348-5069
TransUnion Credit Freeze	**Experian Credit Freeze**	**Equifax Credit Freeze**
P.O. Box 160	P.O. Box 9554	P.O. Box 105788
Woodlyn, PA 19094	Allen, TX 75013	Atlanta, GA 30348-5788

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

You have the right to file/obtain a police report. 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, your state Attorney General, and the FTC.