Exhibit A

DELIVERED VIA EMAIL

Subject line suggestion: CSU Pueblo Cybersecurity Incident

CSU Pueblo community member,

I am writing to inform you of a cybersecurity incident which resulted in the unauthorized access of your personal information.

On August 14, 2024, University employees were the target of a social engineering attack. As a result, an unprotected Excel spreadsheet was accessed by an unauthorized person. This spreadsheet contained the following student information:

- First and Last Name
- Student ID Number
- Current Student Billing Balance

It's important to note that no other personal data was included in this file. Additionally, the attacker did not breach any of the University's or CSU System's computer systems.

The incident only involved the acquisition of this single spreadsheet through manipulative tactics aimed at staff members.

While the exposure was limited, we are providing this information for you to remain vigilant against future social engineering campaigns targeting so you can take steps to protect your personal information.

If you receive any suspicious communication pertaining to financial aid, please confirm that with our **Financial Aid office** at 719-549-2753, financialaid@csupueblo.edu.

If you receive any suspicious communication pertaining to billing, please confirm that with our **Student Billing office** at 719-549-2181.

You may also review your information through your PAWS portal account; however, please remember not to click any links directing you to external websites requesting your personal information such as usernames or passwords. Instead, navigate directly to https://paws.aisweb.csupueblo.edu by typing the address directly into your web browser of choice.

For more information on how to mitigate your personal risk, including contact information for the three major consumer reporting agencies in the US, please visit our CSU System webpage (https://csusystem.edu/cybersecurity).

You can also obtain additional information about fraud alerts and security freezes directly from the credit reporting or website (https://www.ftc.gov), or contacting them via mail at 600 Pennsylvania Avenue, NW, Washington, DC 20580.

If you have any further questions about this matter or about keeping your data safe, please contact the CSU Pueblo IT Help Desk in person or call them at 719-549-2002. You can also submit a Help Desk ticket at https://www.csupueblo.edu/information-technology/help-desk/.

Thank you,
Brandon Bernier
Chief Information Officer, CSU System

Exhibit B

<<Return Mail Address>>

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

<<Notice of Data Breach>>

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

I am writing to inform you of a cybersecurity event at Colorado State University – Pueblo (the "University") that may affect the security of some of your personal information. We are providing you with information about the event, our response, and additional measures you can take to help protect your information, should you feel it appropriate to do so.

What Happened? On August 14, 2024, University employees were the target of a social engineering attack. As a result, an unprotected Excel spreadsheet was obtained by an unauthorized third party. The incident only involved the acquisition of this single spreadsheet. The attacker did not breach any of the University's or the CSU System's computer systems.

What Information Was Involved? The spreadsheet contained the following information related to you:

- First and Last Name;
- CSU ID Number;
- Current Billing Balance.

No other personal data was included in this file.

What We Are Doing. While the exposure was limited, we are providing this information for you to remain vigilant against future social engineering campaigns targeting so you can take steps to protect your personal information.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors for the next twelve to twenty-four months and to report suspected identity theft incidents to the institution. If you receive any suspicious communication pertaining to financial aid, please confirm that with our Financial Aid office at 719-549-2753, financialaid@csupueblo.edu. If you receive any suspicious communication pertaining to billing, please confirm that with our Student Billing office at 719-549-2181.

You may also review your information through your PAWS portal account; however, please remember not to click any links directing you to external websites requesting your personal information such as usernames or passwords. Instead, navigate directly to https://paws.aisweb.csupueblo.edu by typing the address directly into your web browser of choice.

Please also review the enclosed Steps You Can Take to Protect Personal Information, which contains information on what you can do to safeguard against possible misuse of your information.

For More Information. If you have any further questions about this matter or about keeping your data safe, please contact the CSU Pueblo IT Help Desk in person at 2200 Bonforte Blvd, LARC 130, Pueblo, CO 81001-4901, or call them at 719-549-2002, Monday through Friday from 8:00 am to 5:00 pm Mountain time (excluding U.S. holidays). You can also submit a Help Desk ticket at https://www.csupueblo.edu/information-technology/help-desk/.

Sincerely,

Brandon Bernier
Chief Information Officer, CSU System

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

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, tollfree, 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 one-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 Colorado and Illinois residents, you may obtain information from the Federal Trade Commission and the credit reporting agencies about fraud alerts and security freezes.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; 202-727-3400; and oag.dc.gov.

For Iowa residents, you are advised to report any suspected identity theft to law enforcement, including the Federal Trade Commission and the state Attorney General.

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/.

For Massachusetts residents, you have the right to obtain any police report filed in regard to this event. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their 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 consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers 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 consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rightsunder-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov.

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.

For Oregon residents, you are advised to report any suspected identity theft to law enforcement, including the Federal Trade Commission and Oregon Attorney General at Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301- 4096, (877) 877-9392, or www.doj.state.or.us.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. Fees may be required to be paid to the consumer reporting agencies. There are approximately two Rhode Island residents that may be impacted by this event.