Subject line: The Investigation of MCCCD data security incident is now complete

Dear <<Name>>:

We are writing to let you know that Maricopa County Community Colleges District's ("MCCCD") forensic investigation into the March 16, 2021, data security incident is now complete. Please read this email in its entirety for more information on what happened, MCCCD's response and findings, and steps you can take to further protect yourself.

What happened?

On Tuesday, March 16, 2021, the Maricopa County Community Colleges District's (MCCCD) third-party monitoring vendor detected suspicious activity on a system within the network. The information we had at the time suggested it could be a precursor to a cyberattack, which we take very seriously. To protect our systems and data, we immediately implemented our incident response protocols and at the advice of experts, took all systems offline. We hired a team of experts to investigate the suspicious activity and guide us through the containment and restoration process.

What information was impacted?

The forensic investigation determined MCCCD likely identified and prevented a potential ransomware attack, which is largely due to the continued investment in security and training MCCCD has implemented over the past several years.

The investigation also identified an attempt to download a Maricopa directory file which contains the names, dates of birth, email addresses and hashed passwords for Maricopa user accounts. The passwords within the file are hashed, which means the passwords were unreadable without a key to decrypt or break the hash value. However, if you used a commonly known password, it may be possible for an attacker to "crack the hash" and identify your password. The forensic investigation found no evidence the Maricopa directory file left our system, but out of an abundance of caution, we did not permit MCCCD users to access applications unless they changed their password. Included in this email are tips for creating strong and complex passwords, and details on steps that can be taken to further protect your information

It's important to note, the student information and human resources management systems are not hosted within the MCCCD network and were completely unaffected by this incident. **We are confident that no student or employee information from these systems, such as social security numbers, educational information or financial data was compromised as a result of this incident.**

MCCCD has a very large network, with more than 25,000 endpoints, which makes protecting every endpoint a large undertaking. Our security systems and protocols did exactly what they were designed to do – catch potential suspicious activity. Ultimately, our forensic investigators informed us that MCCCD caught and prevented the attack and found suspicious activity on less than 0.1% of systems. Lastly, the investigation found no evidence of any insider wrongdoing.

What we are doing and what you can do:

To increase protections against future incidents, we have accelerated the implementation of new security measures to layer on to the security protocols we had in place prior to March 16th. They include:

- Supplemental 24x7 endpoint detection and threat hunting software
- Additional deployments of multi-factor authentication for all MCCCD employees
- Forced password reset to all MCCCD users, including staff and students.
    - If you have already logged on and completed a password reset, then you do NOT need to do it again.
- Offering complimentary Sophos anti-virus and scanning software for all employees and students for up to ten personal devices

Going forward, we ask that you follow these guidelines relating to usernames/passwords:

- While on the network, do not ask websites or accounts that you visit to remember your password(s).
- You should avoid using your school email address/password combination for any accounts that are not school-related, and do not use your school password for other accounts.
    - If you did, we recommend changing the passwords to those accounts.
- Do not re-use the same password for more than one website or account. Visit the FTC's website for tips and tricks for creating a strong password: h**ps://www.consumer.ftc.gov/blog/2015/07/advanced-password-tips-and-tricks.

In addition, you can find additional information about protecting your identity below:

- It is always a good idea to remain vigilant and monitor your account statements and credit reports as part of your efforts against identity theft. You are entitled to a free credit report every year by law. During COVID, those reports have been freely available on a weekly basis. You can visit the FTC website for more information: h**ps://www.consumer.ftc.gov/articles/0155-free-credit-reports.

- You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report by contacting any one or more of the following national consumer reporting agencies:

Equifax	**Experian**	**TransUnion**
P.O. Box 105139	P.O. Box 2002	P.O. Box 6790
Atlanta, GA 30374	Allen, TX 75013	Fullerton, CA 92834
1-800-685-1111	1-888-397-3742	1-800-916-8800
www.equifax.com	www.experian.com	www.transunion.com

- You may also obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

- **Fraud Alerts:** You can place fraud alerts with the three credit bureaus at one of the three major credit bureaus by phone and also via each credit bureau's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, fraud alerts will now last one year, instead of 90 days. Fraud alerts will continue to be free and identity theft victims can still get extended fraud alerts for seven years.

- **Security Freeze:** A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, each credit reporting agency has a dedicated web page for security freezes and fraud alerts or you can request a freeze by phone or by mail. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request may also require a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. Effective September 21, 2018, placing a freeze on your credit report is now free for all United States citizens.

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion (FVAD)**
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
www.equifax.com	www.experian.com	www.transunion.com

More information can also be obtained by contacting the Federal Trade Commission.

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.identityTheft.gov

Our systems have been successfully restored and are accessible. Even with our improvements, our organization, like all organizations, remains vulnerable to cyber threats. Please remember to always be vigilant against suspicious links and attachments in emails. If an email you receive looks unusual or if you navigate to a site that could be a threat, please immediately contact MCCCD IT here: protectprivacy@domail.maricopa.edu.

For more information:

If you have any questions or concerns, please contact the MCCCD Customer Care Center through live chat with extended availability or you may call 1-877-310-1915 and choose option #5 Monday through Friday from 12 p.m. - 7 p.m. (Pacific Standard Time). Your trust is a top priority for us, and we deeply regret any inconvenience or concern that this matter may cause you.

Sincerely,

James Curtin
Chief Privacy Officer

California Residents may also wish to review the information provided by the California Attorney General at https://oag.ca.gov/idtheft.

New York Residents may obtain additional information about security breach response and identity theft prevention and protection from the New York State Office of the Attorney General at https://ag.ny.gov/ or by calling 1-800-771-7755; the New York State Police at http://troopers.ny.gov/ or by calling 1-518-457-6721; and/or the New York Department of State at https://www.dos.ny.gov or by calling 1-800-697-1220.

Rhode Island Residents may obtain additional information about fraud alerts, security freezes, and steps you can take toward preventing identity theft from the Consumer Protection Division of the Rhode Island Attorney General: Rhode Island Attorney General, Consumer Protection Division, 150 South Main Street, Providence, RI 02903; or by calling 401-274-4400; or visiting www.riag.ri.gov.