

CIPRIANI & WERNER

A PROFESSIONAL CORPORATION

ATTORNEYS AT LAW

KATHLEEN A. MONAGHAN, ESQ.
KMonaghan@c-wlaw.com

450 Sentry Parkway, Suite 200
Blue Bell, PA 19422

Visit us online at
www.C-WLAW.com

Phone: (610) 567-0700
Fax: (610) 567-0712

August 29, 2024

Via EMAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
idtheft@oag.state.md.us

RE: *Data Security Incident Notification*

Dear To Whom It May Concern:

We serve as counsel for South Orange County Community College District ("SOCCCD") located at 28000 Marguerite Parkway, Mission Viejo, CA 92692. We write to provide notification of a recent data security incident. By providing this notice, SOCCCD does not waive any rights or defenses under Maryland law, including the data breach notification statute.

On or around April 5, 2024, South Orange County Community College District ("SOCCCD") became aware of accidental access to an internal SharePoint site by internal district stakeholders. Upon discovery, SOCCCD took immediate action to address the event, including launching an investigation to determine the nature and scope of the event and taking steps to secure its environment. A thorough investigation determined that there was unauthorized access to the information contained within the SharePoint site for a limited period of time. SOCCCD then began a thorough review of the contents of the impacted data in order to determine the type(s) of information contained within the data and to whom that information related. Once this review was completed, SOCCCD immediately worked to obtain up-to-date address information in order to provide individuals with notice.

On August 13, 2024, SOCCCD completed its review and determined the type of information at risk may include first and last name, in combination with a Social Security number. SOCCCD identified approximately three (3) Maryland residents who may have been impacted by this incident.

In response to this incident, SOCCCD immediately took steps to secure its environment, remove access to the SharePoint site, and undertook an investigation. Additionally, SOCCCD provided notice to the potentially impacted individuals on August 29, 2024 via U.S. mail. A copy of the notice is attached as ***Exhibit A***. While SOCCCD has no reason to believe any information has been misused because of this incident; however, in an abundance of caution, SOCCCD is offering potentially impacted individuals 12 months of complimentary credit monitoring and identity protection services.

Very truly yours,

A handwritten signature in black ink, appearing to read "Kathleen Monaghan". The signature is written in a cursive, flowing style.

Kathleen A. Monaghan, Esq.

Exhibit A



August 29, 2024

Dear [REDACTED]:

We write to inform you of a data security event experienced by South Orange County Community College District ("SOCCCD") that may have involved your information as described below. We take the privacy and security of all information very seriously and are providing information about the event, our response, and steps you can take to help protect your information.

What Happened: On or around April 5, 2024, we became aware of accidental unauthorized access to an internal SharePoint site by internal district stakeholders. Meaning, individuals with district authenticated credentials were able to view files with student and employee personal information. Upon discovery, we took immediate action to address the event, including launching an investigation to determine the nature and scope of the event. A thorough investigation determined that there was unauthorized access for a limited period of time. We then began a thorough review of the contents of the impacted data in order to determine the type(s) of information contained within the data and to whom that information related. Once this review was completed, we immediately worked to obtain up-to-date address information in order to provide you with this notice. This process was completed on August 13, 2024, and we worked diligently to provide you with this notification as soon as possible by preparing notification materials and engaging a vendor to provide credit monitoring and identity theft protection for potentially impacted individuals.

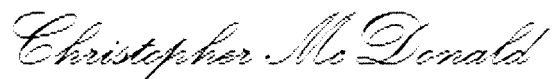
What Information Was Involved: The type(s) of information that may have been contained within the impacted data includes your first and last name, in combination with the following data element(s): [REDACTED].

What We Are Doing: We have taken the steps necessary to address the event and are committed to fully protecting all of the information entrusted to us. Upon learning of this event, we immediately conducted an investigation and took additional steps to secure our environment. Additionally, we are offering you access to complimentary credit monitoring and identity protection services at no charge to you through Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

What You Can Do: We recommend that you remain vigilant against incidents of identity theft and fraud by reviewing your credit reports, account statements, and explanations of benefits documents for suspicious activity and to detect errors. If you discover any suspicious or unusual activity on your accounts, please promptly contact the financial institution or company. We have provided additional information below, which contains more information about steps you can take to help protect yourself against fraud and identity theft, including activating the complimentary credit monitoring and identity protection services we are offering.

For More Information: Should you have any questions or concerns, our dedicated call center can be reached at 1-833-448-2511 from 8:00 am to 8:00 pm Eastern time, Monday through Friday, excluding holidays. Representatives are available for 90 days from the date of this letter. The security of information is of the utmost importance to us. We stay committed to protecting your trust in us and continue to be thankful for your support during this time.

Sincerely,

A handwritten signature in cursive script that reads "Christopher McDonald".

Dr. Christopher McDonald
Vice Chancellor of Educational and Technology Services

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Activate Identity Monitoring Services

In response to the incident, we are providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for twelve (12) months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.



To enroll in Credit Monitoring services at no charge, please log on to [REDACTED] and follow the instructions provided. When prompted please provide the following unique code to receive services:

[REDACTED]

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

00001020280000

Monitor Your Accounts

P

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements and explanation of benefits forms 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 1-800-680-7289 www.transunion.com TransUnion Fraud Alert P.O. Box 2000 Chester, PA 19016-2000 TransUnion Credit Freeze P.O. Box 160 Woodlyn, PA 19094	Experian 1-888-397-3742 www.experian.com Experian Fraud Alert P.O. Box 9554 Allen, TX 75013 Experian Credit Freeze P.O. Box 9554 Allen, TX 75013	Equifax 1-888-298-0045 www.equifax.com Equifax Fraud Alert P.O. Box 105069 Atlanta, GA 30348-5069 Equifax Credit Freeze P.O. Box 105788 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 a police report if you ever experience identity theft or fraud. 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. 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; 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>. South Orange County Community College District may be contacted at 28000 Marguerite Parkway, Mission Viejo, CA 92692.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act: (i) the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; (ii) the consumer reporting agencies may not report outdated negative information; (iii) access to your file is limited; (iv) you must give consent for credit reports to be provided to employers; (v) you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; (vi) and you may seek damages from violators. You 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 you to review your rights pursuant to the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, FTC, 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 Rhode Island residents, the Rhode Island Attorney General may be contacted at 150 South Main Street, Providence, RI 02903; 1-401-274-4400; and www.riag.ri.gov. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There is 1 Rhode Island resident impacted by this incident.

For Washington, D.C. residents, the District of Columbia Attorney General may be contacted at 400 6th Street NW, Washington, D.C. 20001; 202-442-9828, and <https://oag.dc.gov/consumer-protection>. South Orange County Community College District may be contacted at 28000 Marguerite Parkway, Mission Viejo, CA 92692.