



2049 Century Park East, Suite 2900, Los Angeles, CA 90067 • (310) 229-1335

April 1, 2024

Pasha Sternberg
Principal
310.229.1335
psterberg@polsinelli.com

VIA E-MAIL (IDTHEFT@OAG.STATE.MD.US)

Office of the Attorney General
Attn: Jeff Karberg, Administrator of the Identity Theft Program
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, Maryland 21202

Re: Notification of a Data Security Incident

Dear Mr. Karberg:

We represent Clackamas Community College (“CCC”) 19600 Molalla Ave, Oregon City, OR 97045, in connection with a recent incident that may have involved the personal information of three (3) Maryland residents and provide this notice on behalf of CCC pursuant to Md. Code Ann., Com. Law § 14-3504(H). This notice will be supplemented, if necessary, with significant facts subsequently discovered. While CCC is notifying you of this incident, CCC does not waive any rights or defenses relating to the incident, this notice, or the applicability of Maryland law on personal jurisdiction.

NATURE OF THE INCIDENT

Beginning on January 18, 2024, CCC detected encryption on a small number of computer systems and immediately and proactively isolated its network, moved systems offline, and disabled user access. CCC consulted with federal law enforcement and engaged outside forensic experts to investigate the incident. CCC’s investigation determined that an unknown third party accessed certain systems on the CCC network and acquired certain files from CCC’s shared file server. CCC reviewed the files to determine what, if any, personal information may have been involved. On February 29, 2024, CCC determined that the files contained information pertaining to three (3) Maryland residents. The information involved included names and Social Security numbers.

polsinelli.com

Atlanta	Boston	Chicago	Dallas	Denver	Houston	Kansas City	Los Angeles	Miami	Nashville	New York
Phoenix	St. Louis	San Francisco	Seattle	Silicon Valley	Washington, D.C.	Wilmington				

Polsinelli PC, Polsinelli LLP in California



April 1, 2024

Page 2

NOTIFICATION TO THE MARYLAND RESIDENTS

CCC is mailing notification letters to individuals via USPS today, April 1, 2024. CCC is providing an offer for twelve (12) months of complimentary credit monitoring and identity theft protection services. Enclosed is a sample of the notice that CCC is sending to the involved Maryland residents.

STEPS TAKEN RELATING TO THE INCIDENT

Upon learning of the incident, CCC promptly launched an internal investigation and took steps to secure its systems. CCC also engaged a third-party forensic security firm to further investigate the incident and confirm the security of its computer systems. While CCC's security tools were able to contain the issue before it spread throughout the network, out of an abundance of caution, CCC took most of its network offline while it investigated. CCC only brought systems online when CCC's forensic experts deemed them secure.

CONTACT INFORMATION

Please do not hesitate to contact me if you have any questions or if I can provide you with any further information concerning this matter.

Sincerely,

Pasha Sternberg

Enclosure



Return to IDX
P.O. Box 989728
West Sacramento, CA 95798-9728

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

Enrollment Code: <<ENROLLMENT>>

To Enroll, Scan the QR Code Below:



Or Visit:

<https://response.idx.us/clackamascommunitycollege>

April 1, 2024

<<Variable Text 1>>

Dear <<First Name>>,

Clackamas Community College ("CCC") values and respects your privacy, which is why we are writing to advise you of an incident that may have involved some of your personal information. We want to make you aware of the incident and provide you with guidance on what you can do to protect yourself, should you feel it is appropriate to do so.

What Happened. On January 19, 2024, we detected some irregular activity on a small number of computer systems, and quickly determined that an unauthorized third-party gained access to our internal network and encrypted some of our files. We immediately and proactively isolated our network, moved systems offline, and disabled user access. These actions largely prevented the spread of the malicious activity. We also launched an investigation in consultation with federal law enforcement and outside experts specializing in cybersecurity incidents.

What Information Was Involved. The investigation ultimately found that some files from our data server were copied from the network during the incident. We reviewed the contents of these files and, on February 29, 2024, we learned that the files contained your name, <<Variable Text 2>>.

What We Are Doing. As noted above, upon discovering the incident, we activated our incident response plan and launched an investigation in consultation with a team of forensic experts. We also notified federal law enforcement, and we are cooperating with that investigation. We understand that federal and international law enforcement agencies have disrupted the operations of the group responsible for the incident at CCC before any files were publicly released. We are also evaluating additional measures we can take to mitigate the risk of a similar incident from occurring in the future.

Although we are not aware of any instances of fraud or information misuse as a result of the incident, we recommend continuing to remain vigilant and closely monitoring all financial accounts. In addition, we are offering identity theft protection services through IDX, A ZeroFox Company, the data breach and recovery services expert. IDX identity protection services include: 12 months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do. We encourage you to take advantage of the complimentary credit monitoring included with this letter. We encourage you to contact IDX with any questions and to enroll in the free identity protection services by scanning the QR code above, calling 1-888-451-6405, or going to <https://response.idx.us/clackamascommunitycollege> and using the Enrollment Code provided above. You can also find more information on steps to protect yourself against potential fraud in the enclosed *Additional Important Information* sheet. The deadline to enroll is July 1, 2024.

For More Information. We value the trust you place in us to protect your privacy, take our responsibility to safeguard your personal information seriously, and apologize for any inconvenience or concern this incident might cause. For further information and assistance, we have established a dedicated call center to help answer questions you may have about the incident. Please call 1-888-451-6405 from 6:00 a.m. – 6:00 p.m. Pacific, Monday through Friday.

Sincerely,

A handwritten signature in black ink that reads "Tim S. Cook". The signature is written in a cursive, flowing style.

Tim Cook

President, Clackamas Community College

Additional Important Information

As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and monitoring credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission ("FTC").

You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes and steps you can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (1-877-438-4338). You may also contact the FTC at Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Credit Reports: By law, you may obtain a free copy of your credit report once every 12 months from each of the three national credit reporting agencies. The three national credit reporting agencies have also agreed to provide free weekly online credit reports. You can obtain your free credit report by visiting www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at <https://www.annualcreditreport.com/manualRequestForm.action>. Alternatively, you may elect to purchase a copy of your credit report by contacting the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is as follows:

Equifax
1-866-349-5191
www.equifax.com
P.O. Box 740241
Atlanta, GA 30374

Experian
1-888-397-3742
www.experian.com
P.O. Box 2002
Allen, TX 75013

TransUnion
1-800-888-4213
www.transunion.com
P.O. Box 1000
Chester, PA 19016

Fraud Alerts: By law, you have the right to place a fraud alert on your credit report if you believe you have been, or are about to become, a victim of fraud or related crime. A fraud alert is free and will stay on your credit report for one (1) year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at www.annualcreditreport.com/protectYourIdentity.action.

Credit and Security Freezes: By law, you have the right to place a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax Security Freeze
1-888-298-0045
<https://www.equifax.com/personal/credit-report-services/credit-freeze/>
P.O. Box 105788
Atlanta, GA 30348

Experian Security Freeze
1-888-397-3742
<https://www.experian.com/freeze/center.html>
P.O. Box 9554
Allen, TX 75013

TransUnion Security Freeze
1-888-909-8872
<https://www.transunion.com/credit-freeze>
P.O. Box 160
Woodlyn, PA 19094

This notification was not delayed by law enforcement.

Iowa Residents: Iowa residents can contact the Office of the Attorney general to obtain information about steps to take to avoid identity theft from the Iowa Attorney General's office at: Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines IA 50319, 1-515-281-5164.

Maryland Residents: Maryland residents can contact the Office of the Attorney General to obtain information about steps you can take to avoid identity theft from the Maryland Attorney General's office at: Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, <http://www.marylandattorneygeneral.gov/>.

New Mexico Residents: Individuals have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/documents/bcfrp_consumer-rights-summary_2018-09.pdf, or by requesting information in writing from the Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

New York State Residents: New York residents can obtain information about preventing identity theft from the New York Attorney General's Office at: Office of the Attorney General for the State of New York, Bureau of Consumer Frauds & Protection, The Capitol, Albany, New York 12224-0341; <https://ag.ny.gov/consumer-frauds/identity-theft>; 1-800-771-7755.

North Carolina Residents: North Carolina residents can obtain information about preventing identity theft from the North Carolina Attorney General's Office at: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-5-NO-SCAM (Toll-free within North Carolina); 1-919-716-6000; www.ncdoj.gov.

Oregon Residents: Oregon residents are advised to report any suspected identity theft to law enforcement, including the Federal Trade Commission and the Oregon Attorney General. Oregon residents can contact the Oregon Attorney General at 1162 Court St. NE, Salem, OR 97301-4096; 1-503-378-4400; <https://www.doj.state.or.us/>.

Rhode Island Residents: We believe that this incident affected 2 Rhode Island residents. Rhode Island residents can contact the Office of the Attorney general at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov. You have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

Vermont Residents: If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 1-802-656-3183 (1-800-649-2424 toll free in Vermont only).