



Baker&Hostetler LLP

11601 Wilshire Boulevard
Suite 1400
Los Angeles, CA 90025-0509

T 310.820.8800
F 310.820.8859
www.bakerlaw.com

M. Scott Koller
direct dial: 310.979.8427
mskoller@bakerlaw.com

November 11, 2022

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

Brian E. Frosh
Attorney General
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Incident Notification

Dear Attorney General Frosh:

We are writing on behalf of our client, Sierra College (“Sierra”), to notify your office of a security incident. Sierra is a California public community college.

On August 20, 2022, Sierra detected unauthorized access to certain devices in its network that resulted in the encryption of some of its systems. Upon identifying the unauthorized access, Sierra took steps to secure its network and launched an investigation with the assistance of a cybersecurity firm. Sierra also notified law enforcement and is assisting with their investigation.

The investigation was not able to determine the period of unauthorized access but, on October 19, 2022, the investigation determined an unauthorized person accessed files and folders that contained personal information including names, addresses, driver’s license numbers, Social Security numbers, and/or financial account information. Sierra then worked to identify the individuals whose information was accessed as a result of the incident, including seven (7) Maryland residents.

On November 9, 2022, Sierra began mailing notification letters to the Maryland residents

November 11, 2022

Page 2

via U.S. mail in accordance with Md. Code Ann., Com. Law § 14-3504.¹ A copy of the notification letter is enclosed. Sierra is providing a telephone number for potentially affected individuals to call with any questions they may have about the incident. Sierra is offering notified individuals complimentary one-year memberships to identity monitoring services.

To help prevent this type of incident from happening again, Sierra is evaluating additional administrative and technical safeguards.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

A handwritten signature in black ink that reads "M. Scott Koller". The signature is written in a cursive, slightly slanted style.

M. Scott Koller
Partner

Enclosure

¹ This report is not, and does not constitute, a waiver of Sierra's objection that Maryland lacks personal jurisdiction over the company related to this matter.



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

To Enroll, Please Call:

1-833-896-5100

Or Visit:

<https://app.idx.us/account-creation/protect>

Enrollment Code: <<Enrollment Code>>

<<First Name>> <<Last Name>>

<<Address1>>

<<Address2>>

<<City>>, <<State>> <<Zip>>

November 9, 2022

Dear <<First Name>>:

We are writing to notify you that Sierra Joint Community College District ("Sierra College") experienced a security incident that may have involved some of your personal information. This notice explains the incident, what we are doing, and steps you may want to take in response.

What Happened?

On August 20, 2022, Sierra College's network was attacked and some of its systems were encrypted by ransomware. Upon discovery, we took immediate action to secure our network, protect student and employee data and began the restoration process. We also initiated an investigation into the cause and scope of the incident, and a professional third-party forensic firm was engaged to assist.

What Information Was Involved?

On October 19, 2022, our forensic investigation determined that some of your personal information was stored on a computer system that was accessed by an unauthorized individual. That information included names, addresses, passport numbers, driver's license numbers, Social Security numbers, financial account information, and/or medical information.

What We Are Doing.

In an effort to prevent a similar incident from occurring in the future, we have implemented additional measures to enhance the security of our network environment. Additionally, as a precaution, we have arranged to provide identity monitoring at no cost to you through IDX. IDX identity protection services include: 12 months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. For more information on identity theft prevention and IDX Identity Monitoring, including instructions on how to activate your complimentary membership, please see the additional pages provided with this letter.

What You Can Do.

It is always a good idea to remain vigilant by regularly reviewing your financial accounts and credit reports for any unauthorized activity. We also encourage you to enroll in IDX's identity monitoring service. For more information on identity theft prevention and your complimentary services, as well as some additional steps you can take to protect your personal information, please see the additional pages enclosed with this letter.

For More Information.

We regret this incident occurred and apologize for any inconvenience. If you have any questions, please call 1-833-896-5100, Monday through Friday, 6:00 a.m. to 6:00 p.m., Pacific Time.

Sincerely,

A handwritten signature in black ink, appearing to read "Erik Skinner", with a horizontal line extending to the right.

Erik Skinner
Assistant Superintendent
Vice President, Administrative Services



ENROLLMENT INSTRUCTIONS

1. Website and Enrollment. Go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. Please note the deadline to enroll is February 9, 2023.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-833-896-5100 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

If you discover any suspicious items and have enrolled in IDX identity protection, notify IDX immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity over the next 12 to 24 months. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

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

TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

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

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

Experian Security Freeze, PO Box 9554, Allen, TX 75013, www.experian.com

TransUnion Security Freeze, PO Box 2000, Chester, PA 19016, www.transunion.com

Equifax Security Freeze, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

Sierra College is located at 5100 Sierra College Blvd, Rocklin, CA 95677, (916) 624-3333.

Additional information for residents of the following states:

Maryland: You may contact and obtain information from your state attorney general at: *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.oag.state.md.us

New York: may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection*, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, <http://www.dos.ny.gov/consumerprotection>; and *New York State Office of the Attorney General*, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov>

North Carolina: You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov

Rhode Island: This incident involves 1 individual in Rhode Island. Under Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: *Rhode Island Attorney General's Office*, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov