BakerHostetler

Baker&Hostetler LLP

2929 Arch Street
Cira Centre, 12th Floor
Philadelphia, PA 19104-2891

T 215.568.3100
F 215.568.3439
www.bakerlaw.com

Daniel A. Pepper
direct dial: 215.564.2456
dpepper@bakerlaw.com

February 24, 2021

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, Coffeyville Unified School District 445 ("Coffeyville USD" or the "District"), to notify you of a security incident potentially involving one Maryland resident. Coffeyville USD is a school district located in Coffeyville, Kansas.

On August 2, 2020, the District discovered suspicious activity within its network. Upon discovering the incident, the District immediately took steps to secure its digital environment and notified law enforcement. In addition, a cybersecurity firm was engaged, and a thorough investigation was conducted. The investigation determined that there was unauthorized access to certain files on the District's file servers between July 24, 2020, and August 2, 2020. The District completed a careful review of the file servers to identify what information they contained, and on November 30, 2020, the District determined that the files contained the personal information of one Maryland resident, including the resident's name and Social Security number.

Beginning today, February 24, 2021, the District is providing written notice to the Maryland resident by mailing a letter via United States Postal Service First-Class mail.[1] A sample copy of the notification letter is enclosed. The District is offering a complimentary, one-year membership of identity monitoring services provided by Kroll. The District also established a dedicated phone number where the individuals may obtain more information regarding the incident.

[1] This report does not waive Coffeyville USD's objection that Maryland lacks personal jurisdiction over it related to any claims that may arise from this incident.

To help prevent a similar incident from occurring in the future, the District is undertaking a review of how its information is stored and is taking steps to further enhance its existing security measures.

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

Daniel A. Pepper
Partner

Coffeyville, USD 445

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

Coffeyville Unified School District 445 recognizes the importance of protecting information we maintain. We are writing to let you know of an incident that may have involved some of your information. This notice explains the incident, the measures we have taken in response, and some additional steps you may consider taking.

We recently concluded an investigation into an incident involving unauthorized access to our network. Upon discovering the incident, we immediately took steps to secure our digital environment and notified law enforcement. In addition, a cybersecurity firm was engaged, and a thorough investigation was conducted. The investigation determined that there was unauthorized access to certain files on our file servers between July 24, 2020, and August 2, 2020. We completed a careful review of the file servers to identify what information they contained, and on November 30, 2020, we determined the files contained some of your information, including your name and Social Security number.

We wanted to notify you of this incident and assure you that we take it very seriously. It is always advisable to remain vigilant for signs of unauthorized activity by reviewing your financial account statements. If you see charges or activity you did not authorize, we suggest that you contact the provider immediately. As a precaution, we have arranged for you to receive a complimentary one-year membership to identity monitoring services through Kroll. Kroll is a global leader in risk mitigation and response. Your identity monitoring services include Credit Monitoring, Web Watcher, Public Persona, Quick Cash Scan, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration. For more information on identity theft prevention, additional steps you can take in response, and instructions on how to activate your complimentary one-year membership, please see the information provided with this letter.

We regret that this occurred and apologize for any inconvenience. To help prevent something like this from happening again, we are undertaking a review of how our information is stored, and we are taking steps to further enhance our existing security measures. If you have any questions, please call 1-855-914-1991, Monday through Friday, from 8:00 a.m. to 5:30 p.m. Central Time.

Sincerely,

Dr. Craig Correll
Superintendent | Coffeyville Unified School District 445

ACTIVATION INSTRUCTIONS

Visit **https://enroll.idheadquarters.com** to activate and take advantage of your identity monitoring services.

*You have until **May 21, 2021** to activate your identity monitoring services.*

Membership Number: **<<Member ID>>**

Kroll | A Division of DUFF & PHELPS

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you will have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Public Persona

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you will receive an alert.

Quick Cash Scan

Quick Cash Scan monitors short-term and cash-advance loan sources. You will receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to $1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.
To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

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. 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.

Coffeyville Unified School District 445's mailing address is 615 Ellis Street, Coffeyville, KS 67337, and the phone number is 620-252-6400.

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: You 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.