

Dominic A. Paluzzi
Direct Dial: 248.220.1356
E-mail: dpaluzzi@mcdonaldhopkins.com

August 25, 2023

VIA EMAIL (Idtheft@oag.state.md.us)

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

Re: Tucson Unified School District – Incident Notification

Dear Mr. Frosh,

McDonald Hopkins PLC represents Tucson Unified School District (“TUSD”). I am writing to provide notification of an incident that impacted TUSD and may affect the security of personal information of approximately twenty-five (25) Maryland residents. TUSD’s investigation is ongoing, and this notification will be supplemented with any new or significant facts or findings subsequent to this submission, if any. By providing this notice, TUSD does not waive any rights or defenses regarding the applicability of Maryland’s law or personal jurisdiction.

On or about January 20, 2023, TUSD discovered unauthorized access to segments of its network. Upon learning of this issue, TUSD immediately contained the threat by disabling all unauthorized access to its network, notified law enforcement, and commenced a prompt and thorough investigation. As part of its investigation, TUSD worked very closely with external cybersecurity professionals experienced in handling these types of incidents. TUSD conducted a thorough manual review of the data and on or about July 21, 2023, confirmed that the impacted files contained information for residents including full name, Social Security numbers, and health insurance information.

TUSD has no indication that any information has been misused. Nevertheless, out of an abundance of caution, TUSD wanted to inform you (and affected residents) of the incident and to explain the steps that it is taking to help safeguard the affected resident against identity fraud. TUSD is providing the affected residents with written notification of this incident, commencing on or about August 25, 2023, in substantially the same form as the letter attached hereto. TUSD is offering the affected residents complimentary one-year memberships with a credit monitoring service. TUSD is also advising the affected residents about the process for placing fraud alerts and/or security freezes on their credit files and obtaining free credit reports. The affected residents are also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

August 25, 2023

Page 2

At TUSD, protecting the privacy of personal information is a top priority. TUSD is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. TUSD continually evaluates and modifies its practices and internal controls to enhance the security and privacy of personal information.

Should you have any questions regarding this notification, please contact me at (248) 220-1356 or dpaluzzi@mcdonaldhopkins.com.

Sincerely,



Dominic A. Paluzzi

Encl.

TUCSON UNIFIED SCHOOL DISTRICT

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

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

Enrollment Code: [REDACTED]

To Enroll, Scan the QR Code Below:



Or Visit:

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

**<<IMPORTANT INFORMATION
PLEASE REVIEW
CAREFULLY/NOTICE OF DATA
BREACH>>**

August 25, 2023

Dear [REDACTED]

This letter contains important information about a cyber incident in January 2023 that may have disclosed some of your personal information. We want you to understand what happened and to explain the services we are making available to you to minimize the potential impact of this attack. On behalf of Tucson Unified School District (TUSD), I want to assure you that we continue to take significant additional measures to protect the privacy and security of the personal information we maintain and that this effort is of the utmost importance to the district.

What Happened?

Earlier this year, TUSD discovered unauthorized access to segments of our network. We are not alone. It is estimated that at least 48 other school districts have experienced this situation since the beginning of the year, and we are fortunately able to learn from our shared experience to make ever-better provisions for the safety of our information technology systems.

When this incident came to our attention, TUSD immediately contained the threat and notified law enforcement, and with the assistance of experienced external cybersecurity professionals, we began a thorough forensic investigation and manual file review. On July 21, 2023, TUSD learned that the files potentially accessed and/or acquired on or around January 20, 2023, contained some of your personal information.

What Information Was Involved?

The potentially accessed and/or acquired files may have included your personal information, specifically your full name and [REDACTED]

What We Are Doing.

We have enclosed information in this mailing that will help you safeguard against any potential fraud. TUSD has also set up a Call Center to help answer any questions and provide guidance. **You can reach our Call Center's toll-free response line at [REDACTED]** This response line is staffed with professionals who are familiar with this incident, and they are prepared to advise on what you can do to help protect against potential misuse of your information. The response line is available Monday through Friday, 9:00 a.m. to 9:00 p.m. Eastern Time.

What You Can Do.

We have no evidence that any of your personal information has been misused. Nevertheless, out of an abundance of caution, we want to make you aware of the incident. To protect you from potential misuse of your information, we are offering a complimentary membership in identity theft protection services through IDX. IDX identity protection services includes: [REDACTED] 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. For more information on identity theft prevention and IDX identity protection services, including instructions on how to activate your complimentary [REDACTED] month membership, please see the additional information provided in this letter.

This letter also provides other precautionary measures you can take to protect your personal information, including placing a Fraud Alert and/or Security Freeze on your credit files, and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis. To the extent that it is helpful, we have included information about protecting you against medical identity theft.

We remain fully committed to maintaining the privacy of personal information in our possession and have taken a number of additional precautions to safeguard it. We continually evaluate and modify our practices to enhance the security of personal information.

If any additional information concerning this breach becomes available, we will contact you again. Thank you for your active participation in keeping your data safe.

Sincerely,

A handwritten signature in black ink, appearing to read 'Gabriel Trujillo', with a stylized flourish at the end.

Dr. Gabriel Trujillo
Superintendent

– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary [REDACTED] Month Credit Monitoring.

Scan the QR image at the top of this letter or 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. 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. Please note that the enrollment deadline is [REDACTED]

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.

2. Placing a Fraud Alert on Your Credit File.

We recommend that you place an initial 90-day “Fraud Alert” on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax

P.O. Box 740256
Atlanta, GA 30374
<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>
(800) 525-6285

Experian

P.O. Box 9554
Allen, TX 75013
<https://www.experian.com/fraud/center.html>
(888) 397-3742

TransUnion

Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19016-2000
<https://www.transunion.com/fraud-alerts>
(800) 680-7289

3. Placing a Security Freeze on Your Credit File.

If you are very concerned about yourself becoming a victim of fraud or identity theft, you may request a “Security Freeze” be placed on your credit file at no cost. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by sending a request in writing, by mail, to all three nationwide credit reporting companies. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348-5788
<https://www.equifax.com/personal/credit-report-services/credit-freeze/>
(888)-298-0045

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013
<http://experian.com/freeze>
(888) 397-3742

TransUnion Security Freeze

P.O. Box 160
Woodlyn, PA 19094
<https://www.transunion.com/credit-freeze>
(888) 909-8872

In order to place the security freeze, you’ll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving the freeze request, each credit reporting company will send you a confirmation letter containing 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.

If you place a security freeze *prior* to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

4. Obtaining a Free Credit Report.

Under federal law, you may be entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies (if one exists). Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any

accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

5. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations.

6. Protecting Your Medical Information.

The following practices can help to protect you from medical identity theft.

- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.
- Review your "explanation of benefits statement" which you receive from your health insurance company. Follow up with your insurance company or care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential access (noted above) to current date.
- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or the care provider for any items you do not recognize.

* * * * *

Iowa Residents: You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity Theft: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, Telephone: 515-281-5164.

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, <https://www.marylandattorneygeneral.gov/>, Telephone: 888-743-0023.

Massachusetts Residents: Under Massachusetts law, you have the right to obtain a police report 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.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 877-566-7226 (Toll-free within North Carolina), 919-716-6000.

Oregon Residents: You may obtain information about preventing identity theft from the Oregon Attorney General's Office: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.

Washington D.C. Residents: You may obtain information about preventing identity theft from the Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington D.C. 20001, <https://oag.dc.gov/consumer-protection>, Telephone: 202-442-9828.