McDonald Hopkins
A business advisory and advocacy law firm®

RECEIVED
JUL 29 2022
CONSUMER PROTECTION

McDonald Hopkins PLC
39533 Woodward Avenue
Suite 318
Bloomfield Hills, MI 48304
P 1.248.646.5070
F 1.248.646.5075

Dominic A. Paluzzi
Direct Dial: 248-220-1356
E-mail: dpaluzzi@mcdonaldhopkins.com

July 25, 2022

VIA U.S. MAIL

Attorney General John Formella
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Santa Rosa County District Schools – Incident Notification

Dear Attorney General Formella:

McDonald Hopkins PLC represents Santa Rosa County District Schools. I am writing to provide notification of an incident at Santa Rosa County District Schools that may affect the security of personal information of approximately one (1) New Hampshire resident. Santa Rosa County District Schools' 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, Santa Rosa County District Schools does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

On June 25, 2022, Santa Rosa County District Schools discovered that an Excel spreadsheet that contained employee health insurance plan information had been inadvertently posted on its public-facing website and submitted to a third-party vendor's website as part of a Risk Management bid process. On July 8, 2022, Santa Rosa County District Schools' investigation determined that two files containing personal health information were accessed and/or acquired without authorization beginning on or about February 19, 2021. Thereafter, Santa Rosa County District Schools conducted a thorough review of the contents of the files to identify the individuals impacted in connection with the incident. The types of information involved included first and last name, Social Security number, date of birth, and health insurance information.

To date, Santa Rosa County District Schools is not aware of any reports of identity fraud or improper use of any information as a direct result of this incident. Nevertheless, out of an abundance of caution, Santa Rosa County District Schools wanted to inform you (and the affected residents) of the incident and to explain the steps that it is taking to help safeguard the affected residents against identity fraud. Santa Rosa County District Schools is providing the affected residents with written notification of this incident commencing on or about July 25, 2022, in substantially the same form as the letter attached hereto. Santa Rosa County District Schools is offering the affected residents complimentary one-year memberships with a credit

monitoring service. Santa Rosa County District Schools is 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.

Protecting the privacy of personal information is a top priority for Santa Rosa County District Schools. Santa Rosa County District Schools is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. In response to this incident, Santa Rosa County District Schools has conducted a thorough review of its procedures and re-trained employees on the systems that are in place to maintain security of the personal information in its possession. Santa Rosa County District Schools continually evaluates and modifies its practices and internal controls to enhance the security and privacy of its systems.

Notice is being provided pursuant to the HIPAA Breach Notification Rule, 45 CFR §§ 164.400, *et seq.*

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

Sincerely,

Dominic A. Paluzzi

Encl.

SANTA ROSA
COUNTY DISTRICT SCHOOLS
P.O. Box 989728
West Sacramento, CA 95798-9728

To Enroll, Please Call:
1-833-909-4424
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code: <<ENROLLMENT>>

July 25, 2022

<<FIRST NAME>> <<LAST NAME>>
<<ADDRESS1>>
<<ADDRESS2>>
<<CITY>>, <<STATE>> <<ZIP>>
<<Country>>

<<Heading Message>>

Dear <<FIRST NAME>> <<LAST NAME>>:

At Santa Rosa County District Schools, we take the protection of personal information involving employees, students, and others very seriously. We also strongly believe in transparency which is why, as a precautionary measure, we are writing with important information regarding a data security incident involving a file that contained some of your personal information. This letter outlines the details of the incident, how the District has and will continue to respond, and the steps you may want to take to protect your information.

What Happened?

On June 25, 2022, we discovered that an Excel spreadsheet that contained employee health insurance plan information had been inadvertently posted on our Purchasing website on February 19, 2021 and was submitted to a third-party vendor's website as a part of a Risk Management bid process. Upon further investigation, we determined two Excel spreadsheets that contained personal information had been posted in this unauthorized manner. Some of your personal information was included in the Excel files.

What We Are Doing.

Upon learning of the incident, we commenced a prompt and thorough investigation. As part of our investigation, we have worked very closely with external cybersecurity professionals. We immediately took steps to investigate whether there was any potential unauthorized access to the files and to ensure that they were immediately deleted from our website and removed by the third-party vendor in order to mitigate data exposure. Additionally, we notified third-party vendors who may have accessed the information to confirm destruction of the information, to the best of our ability.

Based on the results of our investigation, we believe your personal information was involved in this incident, so we wanted to notify you of the incident and provide you with information on steps you can take to help protect your information. We have no evidence that any of the information has been misused. Nevertheless, out of an abundance of caution, we want to make you aware of the incident.

What Information Was Involved?

The types of information involved included your first and last name, Social Security number, date of birth, and health insurance and ancillary coverage enrollment information. This information did not include personal information such as diagnoses or prescription information.

What You Can Do.

To protect you from potential misuse of your information, we are offering **complimentary** identity theft protection services through IDX. IDX identity protection services include <<12/24>> months of credit and CyberScan monitoring. With this protection, IDX will help you resolve issues if your identity is compromised. To enroll in these services, call [redacted] or go to [redacted] and use the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is October 25, 2022.

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.

For More Information.

We deeply regret and apologize that this disclosure of your data occurred. Although this incident was an isolated one, it is in direct violation of protocols and policies in place. An important part of our response has been a thorough review of the procedures and re-training employees on the systems that are in place to protect your data. We are committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your personal information.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at [redacted]. This response line is staffed with professionals familiar with this incident and knowledgeable 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.

Sincerely,

Dr. Karen Barber
Superintendent

IDX
The Privacy Platform

– OTHER IMPORTANT INFORMATION –

Website and Enrollment Go to [redacted] 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. 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.

Telephone Contact IDX at [redacted] to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

Placing a Fraud Alert

Whether or not you choose to use the complimentary <<12/24>> month credit monitoring services, 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 105069
Atlanta, GA 30348-5069
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

Consider Placing a Security Freeze on Your Credit File

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "Security Freeze" be placed on your credit file. 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

Obtaining a Free Credit Report

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. 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.

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. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

New York Residents: You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; https://ag.ny.gov/consumer-frauds-bureau/identity-theft; Telephone: 800-771-7755.

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, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

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.

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

New Mexico Residents: You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.