Donna Maddux
Partner
4800 Meadows Road, Suite 300
Lake Oswego, Oregon 97035
503.312.6251
dmaddux@constangy.com

October 18, 2024

VIA ONLINE SUBMISSION

Attorney General Anthony G. Brown
Office of the Attorney General
St. Paul Plaza
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Email: idtheft@oag.state.md.us

Re: **Notice of Data Security Incident**

Dear Attorney General Brown:

Constangy, Brooks, Smith & Prophete LLP ("Constangy") represents Central School District 13J. ("CSD), a public school district in Oregon, in connection with the data security incident described in greater detail below. The purpose of this letter is to notify you of the incident in accordance with Maryland's data breach notification statute.

1. Nature of the Security Incident

On February 7, 2024, CSD experienced a network disruption. CSD immediately took steps to secure its network environment and engaged cybersecurity experts to conduct an investigation. The investigation determined that certain files were acquired without authorization on or about February 3, 2024. CSD then conducted a comprehensive review of the affected data to determine whether personal information may have been involved. After a thorough review of the impacted data, on September 20, 2024, it was determined that certain personal information was present in the data set.

2. Number of Affected Maryland Residents & Information Involved

The incident involved personal information for one (1) Maryland resident. The information involved in the incident for the affected Maryland resident included name and health insurance information.

3. Notification to the Affected Individual

On October 18, 2024, a notification letter was mailed to the affected Maryland resident by USPS First Class Mail. The notification letter provides resources and steps this individual can take to help protect their information. The notification letter also offers the individual the opportunity to enroll in 12 months of complimentary identity protection services, including credit monitoring, and identity remediation services, as well as access to a call center, should the individual have questions about the incident. Those services are offered by IDX, a company specializing in fraud assistance and remediation services. A sample notification letter sent to the impacted individual is included with this correspondence.

4. Steps Taken Relating to the Incident

In response to the incident, CSD retained cybersecurity experts and launched a forensics investigation to determine the source and scope of the compromise. CSD also implemented additional security measures to further harden its email environment in an effort to prevent a similar event from occurring in the future. Additionally, CSD has reported the incident to the FBI and will cooperate with any resulting investigation.

Finally, CSD is notifying the affected individual and providing them with steps they can take to protect their personal information as discussed above.

5. Contact Information

CSD remains dedicated to protecting the personal information in its control. If you have any questions or need additional information, please do not hesitate to contact Donna Maddux at dmaddux@constangy.com.

Sincerely,

Donna Maddux
Constangy, Brooks, Smith & Prophete, LLP

Encl.: Sample Notification Letter

Central School District 13J

Return Mail 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:

SCAN ME

Or Visit:
https://app.idx.us/account-creation/protect

October 18, 2024

Subject: Notice of <<Variable Text 2>>

Dear <<Full Name>> <<Last Name>>:

Central School District 13J ("CSD") is writing to inform you of a recent data security incident that may have involved your personal information. CSD takes the privacy and security of all information within its possession very seriously. We are writing to notify you about the incident, provide you with information about steps you can take to help protect your personal information, and offer you the opportunity to enroll in complimentary identity protection services that CSD is making available to you.

What Happened? On February 7, 2024, CSD discovered unusual network activity that disrupted access to certain systems. Upon discovering this activity, CSD immediately took steps to secure our network and launched an investigation with the assistance of independent cybersecurity experts to determine what happened and whether sensitive information may have been affected. The investigation subsequently revealed that certain personal information was acquired without authorization during the incident. On or about September 20, 2024, we completed a comprehensive review of the impacted data containing personal information and determined your information was involved. We then took steps to notify you of the incident as quickly as possible.

What Information Was Involved? The information impacted includes your name and <<Variable Text 1>>.

What Are We Doing? As soon as we discovered this incident, we took the steps described above. In addition, we reported this incident to federal law enforcement and will cooperate with investigative requests as necessary. We also implemented additional security measures to help reduce the risk of a similar incident occurring in the future. We are further notifying you of this event and advising you about steps you can take to help protect your information.

In addition, we are offering you the opportunity to enroll in complimentary identity protection services through IDX – a data breach and recovery services expert. These services include <<12/24>> 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. Please note that the deadline to enroll in these services is January 18, 2025.

What Can You Do? CSD recommends that you review the guidance included with this letter about how to protect your information. You can also enroll in the complimentary identity protection services being offered to you by using the Enrollment Code provided above.

For More Information: Further information about how to help protect your information appears on the following page. If you have questions about this matter or need assistance enrolling in the complimentary services being offered to you, please call IDX at (866) 303-9175 from 6:00 A.M. to 6:00 P.M. Pacific Time, Monday through Friday (excluding holidays).

We take your trust in us and this matter very seriously. Please accept our sincere apologies for any worry or inconvenience that this may cause you.

Sincerely,

Jennifer Kubista

Jennifer Kubista
Superintendent
Central School District 13J

ADDITIONAL STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and monitoring free credit reports closely for errors and by taking other steps appropriate to protect accounts, including promptly changing passwords. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained for remediation assistance or contact a remediation service provider. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC). 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 Ave, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.consumer.ftc.gov, www.ftc.gov/idtheft.

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com/, calling toll-free 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 this form at https://www.annualcreditreport.com/cra/requestformfinal.pdf. You also can contact one of the following three national credit reporting agencies:

Equifax, P.O. Box 740241, Atlanta, GA 30374, 1-800-525-6285, www.equifax.com.
Experian, P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, www.experian.com.
TransUnion, P.O. Box 1000, Chester, PA 19016, 1-800-916-8800, www.transunion.com.

Fraud Alerts: There are two kinds of general fraud alerts you can place on your credit report—an initial alert and an extended alert. You may want to consider placing either or both fraud alerts on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and provide the appropriate documentary poof. An extended fraud alert is also free and will stay on your credit report for seven years. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com. Military members may also place an Active Duty Military Fraud Alert on their credit reports while deployed. An Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment

Credit or Security Freezes: Under U.S. law, you have the right to put a credit freeze, also known as a security freeze, on your credit file, for up to one year at no cost. The freeze will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. There is no fee to place or lift a security freeze. For information and instructions on how to place a security freeze, contact any of the credit reporting agencies or the Federal Trade Commission identified above. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement. After receiving your freeze request, each credit bureau will provide you with a unique PIN or password. Keep the PIN or password in a safe place as you will need it if you choose to lift the 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 via phone, a credit bureau must lift the credit freeze within an hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after receiving your request.

IRS Identity Protection PIN: You can obtain an identity protection PIN (IP PIN) from the IRS that prevents someone else from filing a tax return using your Social Security number. The IP PIN is known only to you and the IRS and helps the IRS verify your identity when you file your electronic or paper tax return. You can learn more and obtain your IP PIN here: https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin.

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include the right to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state attorney general about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the attorney general in your state.

Additional Information:

District of Columbia: The Office of the Attorney General for the District of Columbia can be reached at 400 6th Street, NW, Washington, DC 20001; 202-727-3400; oag@dc.gov; https://oag.dc.gov/

California: The California Attorney General can be reached at: 1300 "I" Street, Sacramento, CA 95814-2919; 800-952-5225; http://oag.ca.gov/

Maryland: The Maryland Attorney General can be reached at: 200 St. Paul Place Baltimore, MD 21202; 888-743-0023; oag@state.md.us or IDTheft@oag.state.md.us; https://www.marylandattorneygeneral.gov/

North Carolina: The North Carolina Attorney General's Office, Consumer Protection Division, can be reached at: 9001 Mail Service Center Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; https://ncdoj.gov/

New York: The New York Attorney General can be reached at: Bureau of Internet and Technology Resources, 28 Liberty Street, New York, NY 10005; 212-416-8433; https://ag.ny.gov/

Texas: The Texas Attorney General can be reached at: 300 W. 15th Street, Austin, Texas 78701; 800-621-0508; texasattorneygeneral.gov/consumer-protection/