Carruth Compliance Consulting is the third-party administrator that handles 403(b) and 457(b) retirement savings plans for many Oregon school districts, including the Sweet Home School District. Carruth recently discovered suspicious activity on their computer systems. An investigation revealed that unauthorized access to Carruth's network occurred in late December 2024, resulting in the compromise of sensitive employee data for Carruth's clients, including SHSD. SHSD systems were not compromised.

This data breach impacts **all employees who have been employed by SHSD since July 2008**, *regardless of whether or not Carruth was actively managing your 403(b) or 457(b) retirement saving plans.*

Here is the Carruth Compliance Consulting Notice of Data Security Event:

Carruth Compliance Consulting ("CCC") is providing notice regarding an event that affected the security of information we maintain on our systems. CCC provides third-party administrative services to public school districts and non-profit organizations for their 403(b) and 457(b) retirement savings plans. We are providing information about the event, our response, and additional measures individuals can take to help protect their information, should they feel it appropriate to do so.

What Happened? On December 21, 2024, CCC identified suspicious activity that impacted the operability of certain computer systems within our environment. Upon becoming aware of the activity, we immediately began working with third-party specialists to investigate the activity, confirm its impact on our systems, and to determine the scope and extent of the information affected by the activity. The investigation determined that certain systems on our network were accessed without authorization between December 19, 2024 and December 26, 2024, and during that time, certain files were copied from our systems. CCC then conducted a review to determine what data was potentially copied without authorization. On January 13, 2025, CCC provided notice of this event.

What Information Was Involved? The information related to individuals that was potentially affected by this event includes their name and a combination of information, including: Social Security number and financial account information. In more limited circumstances, the information could include individuals' driver's license number, W-2 information, medical billing information (but not medical records), and tax filings.

What We Are Doing. The confidentiality, privacy, and security of information in our care is among our highest priorities. When we became aware of this event, we promptly took steps to investigate the activity. Further, we notified the Federal Bureau of Investigation. We are also offering individuals access to credit monitoring and

identity restoration services, through IDX, free of charge. To enroll in credit monitoring, please call IDX at (877) 720-7895.

What You Can Do. CCC encourages individuals to remain vigilant for incidents of identity theft and fraud by monitoring their free credit reports and account activity for suspicious activity, and reporting that activity promptly to their financial institution. Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the credit reporting bureaus. Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below. As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus. Equifax 1-888-298-0045 or www.equifax.com/personal/credit-report-services; Experian 1-888-397-3742 or www.experian.com/help; TransUnion 1-800-916-8800 or www.transunion.com/credit-help.

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state attorney general (information for each attorney general can be found at www.naag.org. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1- 877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on

how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state attorney general.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716- 6000; and www.ncdoj.gov.

For More Information. Individuals with questions regarding this event may call (877) 720-7895, Monday through Friday, from 6:00 am to 6:00 pm Pacific Standard Time, excluding major US holidays.

Last updated January 13, 2025