Constangy Cyber Team
Carruth Compliance Consulting Incident Summary

Dear Colleagues,

Cybersecurity incidents are becoming an unfortunate fact of life. This week we learned that Carruth Compliance Consulting, the third-party administrator of Scio School District's 403(b) and 457(b) retirement plans, experienced a data security incident on December 21, 2024 (the "Carruth Incident" or "Incident"). The affected information at Carruth may include employees' names, Social Security numbers, financial account information, driver's license numbers, W-2 information, medical billing information (but not medical records) and tax filings. The Carruth Incident potentially affects all current and former Scio School District employees back to 2008.

Carruth reported that upon learning of the Incident, they began working with third-party specialists to investigate the activity, and then notified the Federal Bureau of Investigation. Carruth also engaged a sub-contractor to handle processing of information coming in from its clients. **For the foreseeable future, no further retirement account transactions from Scio School District employees will be processed by Carruth.**

Carruth is offering free credit monitoring and identity restoration services to all individuals who may have been affected by the Incident. To enroll in these services, call 877.720.7895. We have requested that Carruth directly notify each affected employee, but you can enroll in the services before receiving an "official" notification letter. We also encourage you to monitor your retirement accounts and consider obtaining a free credit report, and placing an initial or extended fraud alert and/or a credit freeze on your credit file at no cost. **More information about all of these steps is available on our website (LINK)** and more about the Carruth Incident can be found on the Carruth website.

We know receiving this information may be stressful. Please know we are working with Carruth, its insurers and others to understand the full scope of the incident, to ensure all affected employees will be directly notified, and to ensure Carruth is taking appropriate steps to mitigate the impact on our employees.

reported that an investigation revealed that sensitive employee data for Carruth's clients, including Scio School Districtwas affected. Carruth's customers include many Oregon school districts, ESDs and other organizations.

Carruth reported that upon learning of the Incident, they began working with third-party specialists to investigate the activity, and then notified the Federal Bureau of Investigation. Carruth also engaged a sub-contractor to handle processing of information coming in from its

clients. **For the foreseeable future, no further retirement account transactions from Scio School District employees will be processed by Carruth.**

Frequently asked questions

Was my information affected?
It appears that the Carruth Incident may potentially affect all individuals who were employed by Scio School District up to January 2025. We encourage all potentially affected current and former employees to take the steps outlined below to monitor and protect their personal information.

What information was affected?
Carruth reported that the affected information may include employees' names, Social Security numbers, financial account information, driver's license numbers, W-2 information, medical billing information (but not medical records) and tax filings.

What is Scio School District doing?
We are working with Carruth and multiple other parties to understand the full scope of the Incident, to ensure all affected employees will be directly notified and provided appropriate remediation services, and to ensure Carruth is taking appropriate steps to mitigate the impact on our employees. We will update information about the incident as it becomes available.

What should I do?

- **Enroll in credit monitoring and identity restoration services.** Carruth is offering free credit monitoring and identity restoration services through IDX, a firm that provides identity protection services to consumers affected by data security incidents. To enroll, please call IDX at 877.720.7895.
- **Monitor your accounts.** Regularly review your bank accounts, credit card statements, and other financial accounts for any suspicious activity. If you see anything unusual, report it to your financial institution immediately.
- **Check your credit reports.** You are entitled to one free credit report annually from each of the three major credit reporting bureaus (Equifax, Experian and TransUnion). Visit www.annualcreditreport.com or call 877.322.8228 to order your free reports.
- **Consider placing a fraud alert on your credit file.** Fraud alerts notify creditors to verify your identity before issuing new credit. You can place an initial fraud alert (lasting one year), or an extended fraud alert (lasting seven years), at no cost, if you believe you are a victim of identity theft.

Constangy Cyber Team
Carruth Compliance Consulting Incident Summary

- **Consider placing a Credit freeze on your credit file.** Credit freezes prevent credit bureaus from releasing your credit report without your explicit consent. This makes it harder for identity thieves to open accounts in your name. You can place a credit freeze on your credit file at no cost.
- **Report any suspicious activity.** If you suspect you are a victim of identity theft, you should file a police report. You can also report it to the Federal Trade Commission at www.identitytheft.gov or 877.ID.THEFT (877.438.4338).

- **How do I place fraud alerts and credit freezes on my credit file?** Place a fraud alert and/or a credit freeze on your credit file by contacting each of the three major credit reporting bureaus:
  - **Equifax:** 888-298-0045 or https://www.equifax.com/personal/credit-report-services/
  - **Experian:** 888-397-3742 or https://www.experian.com/help/
  - **TransUnion:** 800-916-8800 or https://www.transunion.com/credit-help

Additional resources

- **Federal Trade Commission**: www.identitytheft.gov
- Oregon Attorney General: **www.doj.state.or.us/consumer-protection/id-theft-data-breaches/identity-theft/**