



Donna Maddux, Partner
Cybersecurity & Data Privacy Team
4800 SW Meadows Road, Suite 300
Lake Oswego, Oregon 97035
Telephone: 503.312.6251
Email: dmaddux@constangy.com

February 28, 2025

VIA EMAIL

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: Notification of Data Security Incident

Dear Attorney General Brown:

Constangy, Brooks, Smith & Prophete, LLP represents Pilot Rock School District 2 (“Pilot Rock SD”) in conjunction with their response to the recent Carruth Compliance Consulting incident discussed below. Pilot Rock SD is a public school district located in Pilot Rock, Oregon. The purpose of this letter is to notify you of the incident in accordance with Maryland’s data breach notification statute, Md. Code Ann., Com. Law § 14-3501 et seq.

1. Nature of the Security Incident

On January 13, 2025, Pilot Rock SD was notified by Carruth Compliance Consulting (“Carruth”) that it experienced a data security incident. Carruth provides third-party administrative services for 403(b) and 457(b) retirement plans and monitors contribution compliance for all employees of public schools, community colleges and non-profit organizations.

Pilot Rock SD immediately began an investigation to determine what happened and what data was involved. 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’s investigation determined that personal information may have been acquired without authorization on or about December 21, 2024. However, Carruth could not identify affected individuals.

February 28, 2025

Page 2

Pilot Rock SD then worked to identify all current and former employees whose personal information was shared with Carruth and sufficient contact information for the purpose of notifying them about the incident. That process was completed on February 24, 2025.

2. Number of Affected Maryland Residents & Information Involved

The incident involved personal information for a single (1) Maryland resident. The information involved in the incident may differ depending on the individual but may include the following for the affected Maryland resident: names, Social Security numbers, driver's license numbers, financial account information, and medical billing information.

3. Notification to Affected Individuals

On February 28, 2025, notification letters were sent to affected Maryland residents by USPS First Class Mail.

The notification letter provides resources and steps individuals can take to help protect their information. The notification letter also offers the opportunity to enroll in complimentary identity protection services including 12 months of credit monitoring, dark web monitoring, \$1 million identity fraud loss reimbursement policy, and fully managed identity theft recovery services. A sample notification letter is enclosed.

4. Measures Taken to Address the Incident

Upon discovering this incident, in addition to taking the steps described above, Pilot Rock SD took steps to learn more about what happened and what information could have been affected. Pilot Rock SD has established a toll-free call center through IDX to answer questions about the incident and address related concerns. Finally, Pilot Rock SD notified the potentially affected individuals and provided them with steps they can take to protect their personal information.

5. Contact Information

If you have any questions or need additional information regarding this incident, please do not hesitate to contact me at DMaddux@Constangy.com or 503.312.6251.

Sincerely,



Donna Maddux of
Partner, Constangy Cyber Team

Encl.: Sample Notification Letter



Return Mail Processing Center:
P.O. Box 989728
West Sacramento, CA 95798-9728



816_256667

[Redacted]
[Redacted]
[Redacted]



256667

Enrollment Code: [Redacted]
To Enroll, Scan the QR Code Below:



Or Visit:

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

February 28, 2025

Subject: Notice of Data Security Incident

Dear [Redacted]:

We are writing about a data security incident experienced by Carruth Compliance Consulting (“Carruth”) that may have affected your personal information (the “Carruth Incident” or “Incident”). Carruth provides third-party administrative services for 403(b) and 457(b) retirement plans and monitors contribution compliance for all employees of certain public school districts, community colleges, and non-profit organizations, including Pilot Rock School District. This letter will provide information about the incident, steps you can take to protect your personal information, and the opportunity to enroll in complimentary credit monitoring and identity theft protection services.

What Happened. On January 13, 2025, Pilot Rock School District was notified by Carruth that it experienced a data security incident on December 21, 2024. 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 informed us that its investigation determined that your personal information may have been acquired without authorization on or about December 21, 2024.

What Information Was Involved. The information potentially affected in this Incident may have included your name and a combination of information including your Social Security number and financial account information. In more limited circumstances, the information could include your driver's license number, W-2 information, medical billing information (but not medical records), and tax filings. Carruth reported that if you provided them with the personal information of your beneficiaries, their information may also have been affected in this Incident.

What We Are Doing. As soon as Pilot Rock School District learned about the Incident, we immediately began investigating and sought information from Carruth about the Incident and the impact it may have on our current and former employees’ personal information. We then worked to identify all current and former employees whose personal information was shared with Carruth and sufficient contact information for the purpose of notifying them about the incident.

We are also offering you the opportunity to enroll in complimentary credit monitoring and identity theft protection services through IDX – a data breach and recovery services expert. These services include: 12 months of credit¹ and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery

¹To receive credit monitoring services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

services. With this protection, IDX will help you resolve issues if your identity is compromised. Carruth is also offering any potentially affected individuals, such as a beneficiary, with complimentary credit monitoring and identity theft protection services through IDX. To enroll any beneficiaries, please call IDX at 1-877-390-8299.

What You Can Do. We encourage you to enroll in the credit monitoring and identity protection services we are offering, which are at no cost to you. To enroll, please call 1-877-390-8299 or visit <https://app.idx.us/account-creation/protect> and provide the enrollment code at the top of this page. Please note you must enroll by May 31, 2025. You will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter. Please also review the guidance at the end of this letter which includes additional resources you may utilize to help protect your information. We also encourage your beneficiaries to enroll by calling IDX at 1-877-390-8299.

For More Information. Further information about how to protect your personal information appears on the following page. If you have questions or need assistance, please call 1-877-390-8299 Monday through Friday from 6 a.m. to 6 p.m. Pacific Time.

Sincerely,

Pilot Rock School District
PO Box BB
Pilot Rock, OR 97868
(541) 443-2361
www.pilotrock.k12.or.us



STEPS YOU CAN TAKE TO PROTECT YOUR PERSONAL 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 credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. 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).

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 1-877-322-8228, 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 also can contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105851
Atlanta, GA 30348
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 2000
Chester, PA 19016
1- 833-799-5355
www.transunion.com/get-credit-report

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. 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. 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>.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This 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. 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.

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. Residents of Maryland, New York, North Carolina, Rhode Island and Washington D.C. can obtain more information from their Attorneys General using the contact information below.

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 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; as well as other rights. 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 information:

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.

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

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

North Carolina: 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; www.ncdoj.gov

New York: 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/>

Oregon: Oregon Office of the Attorney General can be reached at: Oregon Department of Justice, 1162 Court St. NE, Salem, OR, 97301, 1-877-877-9392, www.doj.state.or.us

Rhode Island: Rhode Island Attorney General can be reached at: 150 South Main Street Providence, RI 02903, <http://www.riag.ri.gov>.