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

September 6, 2024

NOTICE OF <<[SECURITY INCIDENT] / [DATA BREACH]>>

Dear <<First Name>> <<Last Name>>:

One Point HR Solutions, Inc. ("One Point") writes to inform you of an event involving some of your personal information. Safeguarding information is among One Point's highest priorities, and this letter provides details of the event, our response to it, and resources available to you to help protect your information from possible misuse, should you feel it appropriate to do so.

What Happened? One Point recently became aware of suspicious activity in our email environment. We quickly launched an internal investigation and engaged third-party forensic and data privacy specialists to investigate the nature and scope of the activity. The investigation determined that an unknown unauthorized actor(s) gained access to certain email accounts between July 3, 2023 and February 14, 2024. We then undertook a comprehensive and time-intensive review of the potentially impacted data with the assistance of additional data privacy specialists to identify the information contained within, identify the individuals whose information may have been impacted, and identify accurate address information for potentially impacted individuals. This process is ongoing. One Point is notifying you out of an abundance of caution because, although there is no evidence that the unknown unauthorized actor(s) actually saw or acquired information related to you, the investigation determined that certain information related to you may have been accessed or acquired by an unknown unauthorized actor(s).

What Information Was Involved? Our investigation determined that the following types of personal information may be affected: your <<Variable Text 2>>. Again, One Point is unaware of any attempted or actual misuse of your information.

What We Are Doing. The confidentiality, privacy, and security of information in our care is among our highest priorities. Upon learning of the suspicious activity, we quickly commenced an investigation to investigate the nature and scope of the event. Further, we promptly reported the event to federal and local law enforcement and are cooperating with their investigations. We are reviewing existing security polices and have implemented additional cybersecurity measures to further protect against similar events moving forward. We also reinforced with our staff the importance of safeguarding information in our care and worked with numerous data privacy specialists to assist in the response. Additionally, we undertook a robust effort to review the potentially impacted data to ensure we could notify any potentially impacted individuals, including you, in order to take steps to best protect the information, should they feel it appropriate to do so.

As an added precaution, we are offering you immediate access to credit monitoring and identity theft protection services for <<[twelve (12)/twenty-four (24)]>> months at no cost to you, through IDX, A ZeroFox Company. You can find

information on how to enroll in these services in the enclosed *Steps You Can Take to Protect Personal Information*. We encourage you to consider enrolling in these services as we are not able to do so on your behalf.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. As a best practice you should frequently change your password for all online accounts. If your username and password is potentially impacted by this event, we encourage you to change the passwords, along with the security questions and answers, for all your online accounts. Additionally, please review the information contained in the enclosed *Steps You Can Take to Protect Personal Information.*

For More Information. We understand that you may have questions about this event that are not addressed in this letter. If you have additional questions, please call 1-877-204-0620 from 9:00 a.m. ET to 9:00 p.m. ET, Monday through Friday, excluding major U.S. holidays. You may also write to us at 118 West Fifth Street, Suite 201, Lexington, Kentucky 40508. We take this event very seriously and sincerely regret any inconvenience or concern this event may cause you.

Sincerely,

Ron Heineman, CEO
One Point HR Solutions, Inc.

Steps You Can Take To Protect Personal Information

Enroll in Monitoring Services

1. **Website and Enrollment.** Scan the QR image or go to https://app.idx.us/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. Please note the deadline to enroll is December 6, 2024.

2. 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.

3. Telephone. Contact IDX at 1-877-204-0620 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one (1) free credit report annually from each of the three (3) major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit http://www.annualcreditreport.com or call, toll-free, 1 (877) 322-8228. Consumers may also directly contact the three (3) major credit reporting bureaus listed below to request a free copy of their credit report.

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 one (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 (7) years. Should consumers wish to place a fraud alert, please contact any of the three (3) 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. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two (2) to five (5) years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three (3) major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help/
1 (888) 298-0045	1 (888) 397-3742	1 (800) 916-8800
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect their personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; https://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, the relevant state Attorney General, and the Federal Trade Commission. This notice has not been delayed by law enforcement.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1 (410) 576-6300 or 1 (888) 743-0023; and https://www.marylandattorneygeneral.gov.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting https://www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1 (800) 771-7755; or https://ag.ny.gov.

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 https://www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; https://www.riag.ri.gov; and 1 (401) 274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are approximately 23 Rhode Island residents that may be impacted by this event.