CIPRIANI & WERNER

A PROFESSIONAL CORPORATION

ATTORNEYS AT LAW

Jason Goodwin
jgoodwin@c-wlaw.com

JOHN CLARK
jclark@c-wlaw.com

450 Sentry Parkway, Suite 200
Blue Bell, Pennsylvania 19422

Telephone: (610) 567-0700
Fax: (610) 567-0712

April 12, 2024

Via online submission:
Office of the Maine Attorney General
6 State House Station
Augusta, ME 04333

RE: Notice of Data Security Incident

To Whom It May Concern:

We serve as counsel for SinglePoint Outsourcing, Inc. ("SinglePoint) located at 3300 S. Demaree St. B., Visalia, VA 93277, and provide this notification of a recent data security incident. By providing this notice, SinglePoint does not waive any rights or defenses under Maine law, including the data breach notification statute.

On November 30, 2023, SinglePoint became aware of a potential data security incident and immediately launched an investigation into the nature and scope of the incident with the assistance of third-party specialists. SinglePoint also notified law enforcement. The investigation determined certain data on the SinglePoint network was accessed by an unauthorized individual. SinglePoint conducted a thorough review of the potentially impacted data to determine the type of information contained therein and to whom the information related. SinglePoint completed its review on January 11, 2024 and identified individuals personal information to have been potentially impacted. SinglePoint also began notifying data owners of this incident and worked with those entities to coordinate mailing notification letters to impacted individuals at the direction of the data owners. The type of information potentially impacted included name, Social Security number, driver's license number, and bank account information.

Upon discovery, SinglePoint worked to provide individuals with notification, which included conducting a National Change of Address search to ensure to-to-date address information. SinglePoint began sending individual notification letters on February 8, 2024, via First Class mail, and provided additional notifications on February 28, 2024; March 5, 2024; March 25, 2024; and April 5, 2024. SinglePoint notified 2 Maine resident on behalf of World Wide Sires, Inc., and Golden State YMCA on February 28, 2024 and March 5, 2024. The written notice letters include instructions to access complimentary credit monitoring and identity protection services for 12 months. A copy of the notice letter sent to identified individuals is attached hereto as *Exhibit A*.

In response to this incident, SinglePoint conducted a full forensic investigation, changed passwords, implemented new technical safeguards, including 24/7 managed detection response services, and is continuing to review its policies and procedures related to data protection. As SinglePoint's investigation continues, SinglePoint will supplement this notice should impact to additional Maine residents be identified.

Thank you for your attention to this matter. Please contact me should you have any questions.

Very truly yours,

CIPRIANI & WERNER, P.C.

By: 

Jason Goodwin, Esq.

Exhibit A

SinglePoint Outsourcing
Return Processing Center
4145 SW Watson Avenue, Suite 400
Beaverton, OR 97005

Enrollment Code: <<XXXXXXXX>>

To Enroll, Scan the QR Code Below:

SCAN ME

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

<<First Name>> <<Last Name >>
<<Address 1>><<Address 2>>
<<City>>, <<State>> <<Zip>>

February 28, 2024

<<Notice of Data Breach >>

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

SinglePoint Outsourcing ("SinglePoint") is writing to inform you of an event we experienced that may have impacted certain information as outlined below. SinglePoint was in possession of your information in the regular course of business and in connection with human resource services performed on behalf of <<Business Name>>. This letter includes information about the incident, our response, and resources we are making available to you.

What Happened? On November 30, 2023, we became aware of a potential data incident and immediately undertook an investigation. This included engaging third-party forensic specialists to assist in ensuring SinglePoint systems were secure and conducting a thorough investigation into the nature and scope of the incident. This investigation determined an unauthorized individual acquired certain files between November 8, 2023, and November 9, 2023. Upon discovery, we then conducted a review of the potentially impacted data to determine the type of information contained therein and to whom the information related. <<Variable Sentence 2>>.

What Information Was Involved? The information potentially impacted may have included your first and last name in combination with one or more of the following data elements: Social Security number, date of birth, driver's license number, and/or bank account information.

What We Are Doing. In response to this incident, we reset passwords, secured all accounts, and conducted a full investigation into the incident. We have further implemented additional technical safeguards, including 24/7 system monitoring, to protect SinglePoint systems and help prevent a similar incident from occurring in the future. Additionally, in an abundance of caution, we are offering you access to 12 months of credit monitoring and identity protection services at no cost to you.

What You Can Do. If you have not already, we encourage you to enroll in the complimentary credit monitoring and identity protection services we are making available to you. Information about how to enroll in these services along with additional resources available to you are enclosed.

For More Information. We understand you may have questions about this incident. You may call 1-888-901-3759 between 6 am - 6 pm Pacific Time, Monday through Friday excluding US holidays, or write to us at 3300 S. Demaree St. B, Visalia, CA 93277. We sincerely regret any concern this incident may cause you. The privacy and security of information is important to us, and we will continue to take steps to protect information in our care.

Sincerely,

SinglePoint Outsourcing

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Enroll in Credit Monitoring / Identity Protection

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 May 8, 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 1-888-901-3759 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements for suspicious activity and to detect errors. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

You 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-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

As an alternative to a fraud alert, you 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 your express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

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

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

TransUnion 1-800-680-7289 www.transunion.com **TransUnion Fraud Alert** P.O. Box 2000 Chester, PA 19016-2000 **TransUnion Credit Freeze** P.O. Box 160 Woodlyn, PA 19094	**Experian** 1-888-397-3742 www.experian.com **Experian Fraud Alert** P.O. Box 9554 Allen, TX 75013 **Experian Credit Freeze** P.O. Box 9554 Allen, TX 75013	**Equifax** 1-888-298-0045 www.equifax.com **Equifax Fraud Alert** P.O. Box 105069 Atlanta, GA 30348-5069 **Equifax Credit Freeze** P.O. Box 105788 Atlanta, GA 30348-5788

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement, your state Attorney General, and the FTC. 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; 1-888-743-0023; and www.oag.state.md.us.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act: (i) the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; (ii) the consumer reporting agencies may not report outdated negative information; (iii) access to your file is limited; (iv) you must give consent for credit reports to be provided to employers; (v) you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; (vi) and you may seek damages from violators. You 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 you to review your rights pursuant to the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, FTC, 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 www.ncdoj.gov.

For Washington, D.C. residents, the District of Columbia Attorney General may be contacted at 400 6th Street NW, Washington, D.C. 20001; 202-442-9828, and https://oag.dc.gov/consumer-protection