

CIPRIANI & WERNER

A PROFESSIONAL CORPORATION

ATTORNEYS AT LAW

DANIEL J. HAIER
dhaier@c-wlaw.com

KATIE GORA
kgora@c-wlaw.com

450 Sentry Parkway, Suite 200
Blue Bell, PA 19422

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

www.C-WLAW.com

August 7, 2024

Via Email (idtheft@oag.state.md.us)

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

RE: Security Breach Notification

To Whom It May Concern:

We serve as counsel for OraSure Technologies, Inc. (“OraSure”), located at 220 E 1st Street, Bethlehem, PA 18015. We write to provide notification of a recent data security incident. By providing this notice, OraSure does not waive any rights or defenses under Maryland law, including the data breach notification statute.

On March 27, 2024, OraSure experienced a network disruption and immediately began an investigation with the assistance of third-party specialists. The investigation determined that an unauthorized party accessed certain files on OraSure’s network between approximately March 25 and March 27, 2024.

Therefore, OraSure conducted a thorough review of the files at issue to determine the type of information contained therein and to whom the information related. OraSure determined the data potentially accessed without authorization included names in combination with Social Security number for current and former employees.

At this time, OraSure is aware of information related to approximately 19 residents of Maryland who may have been impacted by this incident.

OraSure notified potentially impacted individuals of this incident via First Class mail on July 9, 2024. A copy of the notice is attached as ***Exhibit A***. OraSure has no reason to believe any information has been misused because of this incident. However, in an abundance of caution,

OraSure is offering the potentially impacted residents of Maryland complimentary access to 12 months of credit monitoring and identity protection services.

In response to this incident, OraSure notified law enforcement and implemented additional network security and data minimization measures. OraSure also continues to review its policies and procedures related to data protection.

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

Very truly yours,

CIPRIANI & WERNER, P.C.

A handwritten signature in black ink, appearing to read 'D Haier', with a stylized flourish at the end.

Daniel Haier, Esq.
610-215-2288
dhaier@c-wlaw.com

OraSure Technologies, Inc
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998



OraSure Technologies, Inc.

P



July 8, 2024

Dear [REDACTED]:

OraSure Technologies, Inc. writes to notify you of an incident that may affect the privacy of certain information related to our employees. This letter includes information about the incident, our response, and resources we are making available to you in an abundance of caution. This letter is a follow-up to the notice we sent to our current employees via email on April 12, 2024 regarding this same incident.

What Happened? On March 27, 2024, we experienced a network disruption that limited our ability to access certain systems on our network. We immediately began an investigation with the assistance of third-party specialists to determine the full nature and scope of the incident. The investigation determined that an unauthorized party accessed certain files on our network between March 25 and March 27, 2024. Therefore, we conducted a thorough review of the files at issue to determine the type of information contained therein and to whom the information related.

What Information Was Involved? Our review determined the files at issue contained human resources information, which potentially included your name in combination [REDACTED]

What We Are Doing. In response to this incident, we notified law enforcement, and we implemented additional network security measures. We also continue to review our policies and procedures related to data protection. We have no reason to believe any information has been or will be misused because of this incident. However, in an abundance of caution, we are providing you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services provide you with alerts for twelve (12) months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company, specializing in fraud assistance and remediation services. These are the same services previously made available to you via email on April 12, 2024.

What You Can Do. If you have not done so already, we encourage you to enroll in the complimentary credit monitoring and identity protection services we have made available to you. Information about how to enroll in these services along with additional resources available to you are included in the attached *Steps You Can Take to Help Protect Your Information*.

000010102G0400

P

For More Information: We understand you may have questions about this incident. You may contact TransUnion at [REDACTED] between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays, or write to us at 220 E 1st Street, Bethlehem, PA 18015.

We regret any concern this incident may cause you and remind you again that we have no reason to believe any information has been or will be misused. The privacy and security of information is important to us and we will continue to take steps to protect information in our care.

Sincerely,

OraSure Technologies, Inc.

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Enroll in Credit Monitoring / Identity Protection

To enroll in Credit Monitoring services at no charge, please log on to [REDACTED] and follow the instructions provided. When prompted please provide the following unique code to receive services: [REDACTED]

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

Once you are enrolled, you will be able to obtain twelve (12) months of unlimited access to your TransUnion credit report and credit score. The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more. The subscription also includes access to identity restoration services that provides assistance in the event your identity is compromised to help you restore your identity and up to \$1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports and 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:



00001020280000

P

TransUnion 1-800-680-7289 www.transunion.com	Experian 1-888-397-3742 www.experian.com	Equifax 1-888-298-0045 www.equifax.com
TransUnion Fraud Alert P.O. Box 2000 Chester, PA 19016-2000	Experian Fraud Alert P.O. Box 9554 Allen, TX 75013	Equifax Fraud Alert P.O. Box 105069 Atlanta, GA 30348-5069
TransUnion Credit Freeze P.O. Box 160 Woodlyn, PA 19094	Experian Credit Freeze P.O. Box 9554 Allen, TX 75013	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. OraSure Technologies, Inc., may be contacted at 220 E 1st Street, Bethlehem PA 18015.

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 Rhode Island residents, the Rhode Island Attorney General may be contacted at 150 South Main Street, Providence, RI 02903; 1-401-274-4400; and www.riag.ri.gov. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are [#] Rhode Island residents impacted by this incident.

For Washington, D.C. residents, the District of Columbia Attorney General may be contacted at 441 4th Street NW #1100, Washington, D.C. 20001; 202-727-3400, and <https://oag.dc.gov/consumer-protection>. OraSure Technologies, Inc., may be contacted at 220 E 1st Street, Bethlehem PA 18015.