

As per state data breach regulations, we are providing you with notice of a breach affecting Maryland residents.

Zenith American Solutions (“ZAS”) experienced a security breach on 9/3/2024. Via a phishing attack, a bad actor gained access to an employee’s email inbox and sub-folders. The personally identifiable information of 2,128 residents of Maryland may have been access by the hacker. ZAS’s Security Department performed a thorough review of our systems to ensure any risk related to this specific phishing event has been addressed, and we have instituted additional security safeguards to prevent re-occurrence. Additionally, the responsible employee has taken additional re-training.

Breach notification letters are being mailed today, and Free Experian IdentityWorks credit monitoring and credit restoration services are being offered at no cost to all affected individuals, and a toll-free line has been provided to assist with any questions.

The personal data that may have been accessed varies with each individual, but potentially includes: name, date of birth, Social Security numbers, birth certificate, marriage certificate, and/or financial/banking information.

Attached is a copy of the letter sent to affected individuals. Please let us know if additional information is needed. Thank you.

Tanya Bowser, CHP | Supervisor, Privacy Compliance

Remote – Illinois | P: (630) 974-4533

Office: 5655 Badura Avenue, Ste. 180, Las Vegas NV 89118

Zenith American Solutions | www.zenith-american.com | [Follow us on LinkedIn](#)

CONFIDENTIALITY NOTICE: The contents of this transmission and any attachments are intended solely for the use of the intended recipient(s) and may contain confidential and/or privileged information that is protected by law. The authorized intended recipient of this transmission is prohibited from disclosing the information contained in this transmission to any unauthorized person(s). If you are not the intended recipient, and you have received this transmission in error, please immediately notify the sender or contact us at 877-217-2676, and then destroy this transmission and any attachments. If you are not the intended recipient, please be advised that any use, sharing, disclosure, distribution, printing, or copying of the contents of this transmission is strictly prohibited. Your cooperation in contacting us of erroneous receipt is appreciated.

From: Bowser, Tanya <TBowser@Zenith-American.com>

Sent: Wednesday, January 29, 2025 1:00 PM

To: IDTheft <IDTheft@oag.state.md.us>

Subject: Breach Notification - Maryland



This is a secure message from Zenith American Solutions

How to open



To read this message on desktop, open the **securedoc_20250129T095942.html** attachment in a web browser.



To read this message on a mobile device, forward this message to mobile@res.cisco.com to receive a mobile login URL.

Need Help?

Contact the sender directly if you are not sure about the validity of this message.

Copyright © 2011-2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.



January 28, 2025

«FirstName» «MI» «LastName» «Suffix»
«ADDRESS» «ADDRESS2»
«CITY» «ST» «ZIP»
«COUNTRY»

RE: Notification of Incident
Reference #: 20240906-175987

Dear «FirstName» «LastName»:

We are contacting you regarding an incident that occurred at Zenith American Solutions, Inc. ("Zenith"), the administrative office for the «ClientName», the "Fund", that may have affected your personal information.

WHAT HAPPENED AND WHAT INFORMATION WAS INVOLVED

On September 6, 2024, we became aware of a sophisticated phishing attack, which resulted in a compromise of a single user's mailbox. The threat actor ("hacker") gained access to an employee's email account for a brief period. During this period, several email folders were accessed by the hacker and some of your personal sensitive information may have been exposed.

The sensitive information that may have potentially been exposed varies by affected individual, but may have included your name, date of birth, Social Security number, birth certificate, marriage certificate, and/or financial/banking information.

WHAT WE ARE DOING

Immediately upon detecting the unusual activity within the email account, we disconnected the hacker's access and reset the employee's credentials and multi-factor authentication to prevent further exposure. The employee was also required to complete phishing prevention retraining. Furthermore, in addition to the phishing prevention tools maintained prior to this incident, Zenith implemented additional phishing tools to reduce the risk of future phishing email attacks. Zenith also contracted with a third party to conduct a thorough analysis to identify the affected individuals and data that may have been exposed. In addition, the matter was reported to law enforcement.

WHAT YOU CAN DO

Although we have no indication that your information was accessed or whether it has or will be misused, we encourage you to take advantage of the «No_Months»-month complimentary identity monitoring and protection services we are making available to you through Experian's® IdentityWorksSM product. If you are interested in these services, please contact us at (855)619-0890 within 30 days of the date of this letter.



Also, please review the enclosed document, which describes additional steps you can take to help safeguard your information, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

FOR MORE INFORMATION

If you have additional questions or concerns regarding this matter, please do not hesitate to contact us at (855)619-0890. We want to assure you that we take great measures to protect your privacy and are committed to providing quality service. We apologize for this incident and any inconvenience it may cause you.

Sincerely,

Privacy Department

ZENITH AMERICAN SOLUTIONS, INC.

Additional Information to Help Safeguard Your Information

Monitoring: It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

Credit Reports: You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348 1-800-349-9960 https://www.equifax.com/personal/credit-report-services/credit-freeze/	Experian Security Freeze P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/center.html	TransUnion Security Freeze P.O. Box 160 Woodlyn, PA 19094 1-800-909-8872 www.transunion.com/credit-freeze
---	---	--

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with:

- Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf);
- TransUnion (<https://www.transunion.com/fraud-alerts>); or
- Experian (<https://www.experian.com/fraud/center.html>).

A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years.

File Police Report: You have the right to file or obtain a police report if you experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.

FTC and Attorneys General: You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General. Federal Trade Commission - Consumer Response Center: 600 Pennsylvania Ave, NW, Washington, DC 20580; 1-877-IDTHEFT (438-4338); www.identitytheft.gov, 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. You can obtain further information on how to file such a complaint by way of the contact information listed above. 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.

- **Arizona Residents:** Contact the Arizona Office of the Attorney General Consumer Protection & Advocacy Section at - 2005 North Central Avenue, Phoenix, AZ 85004 1-602-542-5025.
- **California Residents:** Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.
- **Colorado Residents:** Contact the Colorado Office of the Attorney General Consumer Protection at - 1300 Broadway, 9th Floor, Denver, CO 80203 1-720-508-6000 www.coag.gov.
- **DC Residents:** Contact the District of Columbia Office of the Attorney General at – Office of Consumer Protection: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; www.oag.dc.gov.
- **Illinois Residents:** Contact the Illinois office of the Attorney General at - 100 West Randolph Street, Chicago, IL 60601; 1-866-999-5630; www.illinoisattorneygeneral.gov.
- **Iowa Residents:** State law advises you to report any suspected identity theft to law enforcement or to the Attorney General. Contact Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, Telephone: 515-281-5926 or 888-777-4590 for residents outside of Des Moines.
- **Kentucky Residents:** Contact the Office of the Attorney General of Kentucky at - 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.
- **Maryland Residents:** Contact the Office of the Attorney General of Maryland, Consumer Protection Division at - 200 St. 16th Floor, Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.
- **Massachusetts Residents:** It is required by state law that you are informed of your right to obtain a police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

- **New Mexico Residents:** State law advises you to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach. You have rights pursuant to the Fair Credit Reporting Act ("FCRA"), 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 FCRA, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit your "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the FCRA not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the FCRA. We encourage you to review your rights pursuant to the FCRA by visiting: 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, DC 20580.
- **New York Residents:** the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.
- **North Carolina Residents:** Contact the Office of the Attorney General of North Carolina at - 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.
- **Oregon Residents:** State law advises you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission. You may obtain information about preventing identity theft from the Oregon Attorney General's Office: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392
- **Rhode Island Residents:** Contact the Office of the Attorney General at - 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400. It is required by state law that you are informed of your right to file or obtain a police report in regard to this incident.
- **Vermont Residents:** If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-2424).
- **West Virginia Residents:** You have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described above. You also have a right to place a security freeze on your credit report, as described above.