

WHITEFORD, TAYLOR & PRESTON L.L.P.

SEVEN SAINT PAUL STREET
BALTIMORE, MARYLAND 21202-1636

MAIN TELEPHONE (410) 347-8700
FACSIMILE (410) 752-7092

RAZVAN E. MIUTESCU
PARTNER
DIRECT LINE (410) 347-8744
DIRECT FAX (410) 223-3725
RMiutescu@whitefordlaw.com

DELAWARE*
DISTRICT OF COLUMBIA
KENTUCKY
MARYLAND
NEW YORK
VIRGINIA

WWW.WHITEFORDLAW.COM
(800) 987-8705

December 16, 2024

VIA ELECTRONIC MAIL

(IDTheft@oag.state.md.us)

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

RE: Notification of Data Security Incident

To Whomever It May Concern:

We represent the American Humanist Association (“AHA”), a small non-profit organization with its principal office at 1821 Jefferson PI NW, Washington, DC 20036, in connection with an incident that may have affected the personal information of **nineteen (19)** Maryland residents.

AHA is reporting this incident pursuant to Md. Code Ann., Com. Law § 14-3504(h). This notice will be supplemented, if necessary, with any new significant facts discovered subsequent to this submission. AHA is continuing to engage in data mining of certain files and, if warranted by new findings, will make notifications on a rolling basis.

While AHA is notifying the Office of the Attorney General of Maryland of this incident, AHA does not waive any rights or defenses relating to the incident, this notice, or the applicability of Maryland law on personal jurisdiction.

Nature of the Incident

On September 30, 2024, AHA suffered a ransomware attack to on-premise computer systems. Although it is not known with certainty whether the bad actor, in fact, acquired information from the affected on-premise computers, AHA inferred this conclusion based on information revealed during the investigation of the incident.

On October 28, 2024, based on on-going data mining performed by AHA with assistance and guidance from counsel and a data mining vendor, AHA discovered that certain personal information of the Maryland residents was affected by this incident,

December 16, 2024

Page 2

including first name, last name, Social Security Number (SSN), driver's license number (DLN) and/or tax return information, such as income and withholdings.

Notice to Maryland Residents

Today, December 16, 2024, AHA is providing notice to all Maryland residents affected by the incident. Law enforcement did not delay the sending of this notification. The notification letters include an offer of eighteen (18) months of complimentary credit monitoring and identity theft protection services. Enclosed is a copy of the notice that is being sent to the Maryland residents via first-class United States mail.

Steps Taken Relating to the Incident

Immediately after the ransomware attack occurred on September 30, 2024, AHA has initiated an internal investigation and undertook remedial actions, including rebuilding the affected servers and reinstating data from back-up; engaging counsel and consulting with a cybersecurity forensics firm; and consulting with a data mining company to identify personal information potentially affected. The data mining of the copies of the affected files is ongoing.

AHA is in process of updating its policies and procedures to a more comprehensive written information security policy, including with respect to encryption of data, password security, and multi-factor authentication requirements. AHA will be engaging in employee training through a proactive phishing vulnerability testing and continuing cybersecurity awareness program, monthly information technology (IT) meetings, and migrating on-premise data to a cloud solution.

Contact information

Please do not hesitate to contact me if you have any questions or if we can provide further information concerning this matter.

Very truly yours,

A handwritten signature in blue ink, appearing to read 'Razvan E. Miutescu', with a stylized flourish at the end.

Razvan E. Miutescu
Partner

Enclosure

Dec. 6, 2024

Via First Class Mail

«Name»

«Address»

«City_State_Zip»

RE: Notice of Data Incident

Dear «Name»,

I am writing to inform on behalf of the American Humanist Association (the “Association”) that we have been investigating and monitoring a data breach.

On October 28, we learned that a threat actor may have obtained access to and acquired information in our on-premise computer systems. The information affected included certain of your personal information, including first name, last name, Social Security Number (SSN), driver’s license number (DLN) and/or tax return information, such as income and withholdings. After an initial ransomware attack we suffered on September 30, 2024, we investigated internally and also consulted cybersecurity forensics experts to assist with the investigation of the attack. We are not absolutely certain that your specific information was, in fact, acquired by the threat actor, but we inferred this conclusion based on information revealed during the investigation and after a review of our files that may have been affected.

We will be reaching out to employees for training through a proactive phishing vulnerability testing and continuing cybersecurity training, monthly information technology (IT) meetings, and migrating on-premise data to a cloud solution. We are also emphasizing to all our employees to follow the Association’s procedures for email account password protection and multi-factor verification carefully.

Since the incident, we have rebuilt the affected server and are working on implementing a secure systems restoration strategy, assessed the availability, completeness, and integrity of existing backups or recovered data, recovered data and systems, and securely configured restoration networks. We are updating to a more formal and comprehensive written information security policy overall, including with respect to encryption of data, password security, and multi-factor authentication requirements.

We are offering free credit monitoring services that you can elect to enroll in for a period of 18 months. This is a service you may choose at no cost to you to protect you against identity theft consequences as a precaution.

In addition to enrolling in the complimentary identity theft protection services being offered, you can review the enclosed *Additional Important Information* for additional information on steps you can take to protect against identity theft and fraud.

We regret any inconvenience this may cause you and we are sorry for having to send this notification. If you have any questions regarding this notice, please contact us by email at aha@americanhumanist.org, by telephone at (800) 837-3792, or write to us at 1821 Jefferson Pl. NW, Washington, DC 20036.

Sincerely,

Joaquin Cabrejas
Comptroller
American Humanist Association

Additional Important Information

For residents of Hawaii, Michigan, Missouri, North Carolina, Vermont, Virginia, and Wyoming: It is recommended by state law 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.

For residents of Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon, and West Virginia:

It is required by state laws to inform you that 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.

For residents of Vermont: 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 802-828-3171 (800-649-2424 toll free in Vermont only).

For residents of New Mexico: Individuals interacting with credit reporting agencies have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/documents/bcfc_consumer-rights-summary_2018-09.pdf, or by requesting information in writing from the Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

For Residents of Washington, D.C.: You can obtain information about steps to take to avoid identity theft from the Office of the Attorney General for the District of Columbia at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; www.oag.dc.gov.

For residents of Iowa: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Oregon: State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Maryland, Rhode Island, Illinois, New York, and North Carolina: You can obtain information from the Maryland and North Carolina Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft

Maryland Office of the Attorney General Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202 1-888-743-0023 www.oag.state.md.us

Rhode Island Office of the Attorney General Consumer Protection, 150 South Main Street, Providence, RI 02903 1-401-274-4400 www.riag.ri.gov

North Carolina Office of the Attorney General Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001 1-877-566-7226 www.ncdoj.com

Federal Trade Commission Consumer Response Center, 600 Pennsylvania Ave, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) www.ftc.gov/idtheft

New York Office of Attorney General Consumer Frauds & Protection, The Capitol, Albany, NY 12224 1-800-771-7755 <https://ag.ny.gov/consumer-frauds/identity-theft>

For residents of Massachusetts and Rhode Island: It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

For residents of all states:

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. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

..

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
equifax.com/personal/credit-report-services/
1-888-Equifax (1-888-378-4329)

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013
experian.com/freeze/center.html
1-888-397-3742

TransUnion Security Freeze

P.O. Box 160
Woodlyn, PA 19094
transunion.com/credit-freeze
1-833-395-6938

More information can also be obtained by contacting the Federal Trade Commission listed above.

..