

Good afternoon,

Attacker gained access to Alan Ritchey, Inc.'s Domain Computer and Servers, encrypted and locked them out of access beginning early morning February 6, 2024 at 04:30 AM Central Time. IT was called by their dispatch of a system malfunction. Upon their arrival at the site, their servers were nonfunctional, and a ransom text file was discovered in the folders from the unauthorized user. Since they had intact off-site copies, their systems have been restored using those and no contact was made with the attackers. The FBI was notified February 14, 2024. Third-party cyber forensics was obtained, and they ascertained information was exfiltrated January 29, 2024. Continued internal review of the data was completed April 1, 2024 that fully identified affected individuals. In total 12,885 individuals' names, along with social security numbers and driver's license numbers were exfiltrated. This included one (1) Maryland resident.

To mitigate future occurrences, Alan Ritchey, Inc. has increased their technical security. Attached is the draft notification letter we anticipate will be mailed next week.

Please let us know if any further information is needed. Thank you kindly.
Christine

Christine A. Chasse RN, JD, MSN, NE-C, CIPP/US | Associate
Spencer Fane LLP

2200 Ross Ave, Suite 4800 | Dallas, TX 75201
O 214.459.5884 M 817.773.8165
cchasse@spencerfane.com | spencerfane.com



<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

<<Date>>

Enrollment Code: <<XXXXXXXX>>

To Enroll, Scan the QR Code Below:



Or Visit:

<https://response.idx.us/customending>

Notice of Data Breach

Dear <<First Name>> <<Last Name>>,

We are contacting you regarding a data security incident that occurred on February 6, 2024 when an unauthorized user accessed Alan Ritchey, Inc. ("Alan Ritchey") server. As a result of this security incident, some of your personal information was exposed to others. Therefore, out of an abundance of caution, we are notifying you of this incident.

What Happened

In the early morning hours of February 6, 2024, we recognized an unauthorized user was on our server. We quickly terminated their access, notified law enforcement and obtained a reputable third-party forensics vendor to analyze the scope of their unauthorized access. On February 29, 2024, after learning more information through the investigation into this security incident, Alan Ritchey discovered that certain personally identifiable information was contained within the server. We have been diligently working through this supplied information and further determined your information was included. We are notifying you of this incident at this time.

What Information Was Involved

Although the specific information that was contained within the server varies by individual, such information may include: first and last name, address, date of birth, phone number, address, Social Security number, passport number, driver's license number, birth certificate, and drug test results.

What We Are Doing

At Alan Ritchey, we take the responsibility of maintaining non-public information seriously. We have, and will continue to, implement additional security controls to reduce the risk of a similar incident occurring again. In addition, we are offering identity theft protection services to all impacted adults through IDX, A ZeroFox Company, the data breach and recovery services expert. IDX identity protection services include: 12 months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do

We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling [TFN], going to <https://response.idx.us/customending>, or scanning the QR image and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 8 am - 8 pm Central Time. Please note the deadline to enroll is [Enrollment Deadline].

Again, at this time, we are not aware of any additional evidence indicating that your information has been used for fraudulent purposes. However, we encourage you to take full advantage of this service offering.

For More Information

You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

We deeply regret that this has occurred and apologize for any inconvenience or concern caused by this incident. Please call [TFN] if you'd like to speak to someone. Alternatively, you may go to <https://response.idx.us/customending> for assistance or for any additional questions you may have.

Sincerely,

Robby Richey

Robby Richey
Chief Executive Officer
Alan Ritchey, Inc.

(Enclosure)



Recommended Steps To Help Protect Your Information

1. Website and Enrollment. Scan the QR image or go to <https://response.idx.us/customending> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

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 [TFN] 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.

You should also know that you have the right to file a police report if you ever 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 some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. 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. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

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, 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 "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. 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. You can review your rights pursuant to the Fair Credit Reporting Act 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, D.C. 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: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 1-877-877-9392

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, <https://consumer.ftc.gov>, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.