America Job Link Alliance Data Incident

Frequently Asked Questions

March 22, 2017

Q: What happened?

On February 20, 2017, a hacker created a job seeker account in an America's JobLink (AJL) system. The hacker then exploited a vulnerability in the application code to gain unauthorized access to certain information of other job seekers. This vulnerability has since been eliminated.

America's Job Link Alliance–Technical Support (ALJA–TS) first noticed unusual activity in AJL via system error messages on March 12. AJLA–TS immediately notified law enforcement, retained an independent forensic firm to investigate the cause and scope of the activity, and secured the application code.

Q: What personally identifiable information was the hacker able to see?

The personally identifiable information included users' names, dates of birth, and Social Security numbers.

Q: Which states were affected?

The hacker was found to have activity in the AJL systems of ten states: Alabama, Arkansas, Arizona, Delaware, Idaho, Illinois, Kansas, Maine, Oklahoma, and Vermont.

Q: Is the JobLink site now safe to use?

The vulnerability was identified and eliminated on March 14 and no longer poses a threat to the AJL systems.

Q: Is law enforcement involved?

Yes. AJLA–TS contacted law enforcement immediately and is currently working with the FBI to identify and apprehend the hacker.

Q: How did this happen?

The vulnerability was introduced in an AJL system update in October 2016.

Q: Does the vulnerability or the hacker pose a threat to the ReportLink or CertLink users?

No. The vulnerability did not pose a threat to the ReportLink or CertLink systems and users.

Q: Why do you need Social Security numbers in the first place?

The federal government requires that we ask for your Social Security number. As the AJL system indicates, however, you are not required to provide it.

Q: I've read news stories online about a virus. Was a virus involved?

No. This incident did not involve a virus or any other form of malware.

Q: If AJLA–TS knew about this incident on March 12, why am I only learning about this now?

Notifying potentially affected individuals has been a top priority since AJLA–TS discovered that the error messages we were receiving were due to malicious activity and not a technical issue. Before releasing a public announcement, however, it was important that AJLA–TS identify the vulnerability and eliminate it from the system. The forensic firm's analysis required the review of a significant amount of system data. This analysis was needed to confirm that the hacker had actually accessed individuals' information, so as not to unnecessarily alarm affected individuals. Finally, it was critically important that any announcement not interfere with law enforcement's investigation.

Q: Do you suspect that my information has been used fraudulently?

We do not have any evidence that your information was actually misused, but we take our obligation to protect your information seriously and wanted to ensure that you received notification as soon as possible.

Q: I would like to receive free credit monitoring or other identify theft protection.

While we do not have evidence that your information was misused, job seekers should remain vigilant with respect to reviewing bank, credit card, and debit card account statements and report any suspicious activity to your bank or credit company.

We recommend monitoring credit reports with the major credit reporting agencies listed below:

Equifax	Experian	TransUnion
1 800 685-1111	1 888 397-3742	1 800 916-8800
PO Box 740241	PO Box 2104	PO Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19022
www.equifax.com (link is external)	www.experian.com (link is external)	www.transunion.com (link is external)

You may request that they place a fraud alert and or a credit freeze on your file. You may also contact the IRS Identity Protection Specialized Unit at 1-800-908-4490. See identitytheft.gov/databreach for additional follow-up steps.

Q: Who can I contact with additional questions?

You may contact us with any additional questions about the incident at AJLAincidentresponse@AJLA.net.