Notice of Data Security Incident

Alcott is providing notice of a security incident via this posting. There is ***no*** evidence that any information has been or will be misused because of this incident. The security of information is very important to us, and we sincerely apologize for any inconvenience this may cause. Alcott may have had your data if you participated in an Alcott program.

What Happened?

In February 2025, Alcott noticed unusual activity on some of its systems. We immediately implemented our incident response protocols, reported the circumstances to law enforcement, and engaged independent computer forensic experts to assist with conducting a thorough investigation. The investigation determined that an unauthorized user gained access to some of Alcott's systems where information was stored. In March of 2026, we completed our review of the information and determined that an unauthorized user gained access to Alcott's systems where information was stored. Alcott has not found evidence that any such information has been misused.

Alcott's human capital management platform, iSolved, which collects and stores employee information like tax forms, benefits enrollment, and banking information, was **not** impacted in the event.

What Information Was Involved?

The categories of information impacted could include your name, date of birth, Social Security number, driver's license information, health information, and/or other information provided to Alcott in connection with its services.

What We Are Doing:

We have taken steps to prevent this kind of event in the future, such as improving our vendor support and security, enhancing threat detecting and endpoint monitoring tools utilized in our IT environment, strengthening firewalls, conducting third-party review of our configuration details, reemphasized password and multifactor authentication policies, and working with our IT and security experts to further enhance our security posture. Finally, Alcott took steps to prevent any personal information from being released publicly.

In addition, although there has been no evidence your information was misused, we are offering identity theft protection services through Cyberscout, a TransUnion Company, specializing in fraud assistance and remediation services for 24 months. With this protection, Cyberscout, will help you resolve issues if your identity is compromised.

What You Can Do:

We encourage you to contact Cyberscout with any questions and to enroll in the free identity protection services by calling 1-844-507-4934. Cyberscout representatives are available Monday through Friday from 8 a.m. - 8 p.m. Eastern Time. Please note the deadline for enrolling is September 15, 2026.

This notice also provides other precautionary measures you can take to protect your information. Additionally, you should always remain vigilant in reviewing your account statements and credit reports for fraudulent or irregular activity on a regular basis.

For More Information:

If you have questions, please call 1-844-507-4934, Monday through Friday from 8 a.m. to 8 p.m. Eastern Standard Time. Protecting your information is important to us, and we sincerely apologize for any concern this incident may cause you.

Sincerely,

The Alcott Team

Recommended Steps to help Protect your Information

1. **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.

   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.

2. **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	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	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.

3. **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.

4. **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.

District of Columbia Residents: Office of the Attorney General, 400 6th Street, NW, Washington, DC 20001; 202-727-3400; oag@dc.gov.

Iowa Residents: Office of the Attorney General, 1305 E. Walnut Street, Des Moines, Iowa 50319; 515-281-5926; consumer@ag.iowa.gov.

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.

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

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.

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

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.