SENIOR OPERATIONS LLC
300 East Devon Avenue
Bartlett, Illinois 60103
U.S.A.

March 5, 2026

Notice of Data Breach

Dear Recipient,

Senior Aerospace Jet Products and Ketema, formerly a division of Senior Operations LLC ("Senior"), is writing to inform you of a data security incident that may have resulted in unauthorized access to your personal information. We are providing you with details of the incident, steps we are taking in response, and resources available to help you protect against the potential misuse of your information. Please be assured that Senior takes the protection and proper use of your personal information very seriously.

What Happened?
In late December 2025, Senior identified and responded to an attempted ransomware incident that impacted the Senior Aerospace Jet Products/Ketema environment. At the time of the incident, the attack was believed to have been successfully prevented by Senior's security controls, with no evidence of data compromise. However, as part of the ongoing investigation and additional forensic analysis to determine the scope of the breach, which was completed in late February 2026, Senior identified that the attacker was able to access files containing Personally Identifiable Information ("PII"). Senior is partnering with leading cybersecurity experts to implement successful remediation activities and ensure the attack is fully contained.

What Information was Involved?
The accessed personal information may include your name, address, Social Security Number, date of birth, passport number, driver's license number, other government identification card, and potentially previously submitted medical information or partial banking information related to direct deposit. Currently, we do not believe that any individual's personal information has been misused.

What We are Doing:
Upon detecting the intrusion, Senior promptly initiated preventative measures to mitigate further data loss and contain the incident. Ongoing investigation encompassed comprehensive forensic analysis and the implementation of additional robust safeguards to enhance data security and safeguard against future criminal activity.

In addition, we are providing you with the option of identity and/or credit monitoring protection services through a third-party provider for one (1) year at no cost to you. Current and former employees should contact Sharon Sundt, Director of Benefits & HRIS US, at IDHelpLine@seniorplcusa.com or 630.540.5220 **no later than May 15, 2026,** to request and activate your identity monitoring services.

What You Can Do:
We encourage you to enroll in the free identity protection services Senior is offering. We also encourage you to periodically check your credit reports to ensure that no fraudulent activity has occurred. Even if there are no signs of fraud in these reports, we recommend that you remain vigilant, continue to check these credit reports and your account statements periodically, and report anything suspicious to law enforcement.

Please read further below to review recommendations from the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert and/or security freeze on your credit file.

At this time, Senior has no evidence that your information has been misused. However, we encourage you to take full advantage of all available services.

For More Information:
Keeping your personal information secure is of the utmost importance to Senior. We sincerely regret any concern or inconvenience this event may cause you. Should you have any questions regarding this letter, please contact me or Sharon Sundt, Director of Benefits & HRIS US; IDHelpLine@seniorplcusa.com; 630.540.5220

Thank you for your time and attention to this important matter.

Sincerely,

Emi Donis

Emi Donis
General Counsel, North America
Senior Operations LLC
Email: edonis@seniorplcusa.com

Recommended Steps to Help Protect Your Information

1. **Website and Enrollment.** Please follow the instructions in the letter sent to you directly by our third-party identity protection provider.

2. Activate the credit monitoring provided as part of your identity protection membership. The monitoring included in the membership must be activated to be effective.

3. 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.

4. 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.**

5. 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.

6. You can obtain additional information about the steps you can take to avoid identity theft from the Federal Trade Commission. The Federal Trade Commission encourages those who discover that their information has been misused to file a complaint with them. For all US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.