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

November 20, 2020

Office of the Washington Attorney General
Consumer Protection Division
1125 Washington Street SE
PO Box 40100
Olympia, Washington 98504

Delivered via email to SecurityBreach@atg.wa.gov

Subject: Data Security Incident Notification

Dear Sir or Madam:

I am writing on behalf of Senior Operations LLC ("Company"), doing business in the state of Washington as Senior Aerospace AMT and Damar AeroSystems. We are writing to notify you of a data security incident.

In late October 2020, the IT systems of AMT and Damar experienced a broad ransomware attack. On October 24, 2020, the Company took action to shut down all of AMT and Damar's IT systems to mitigate the extent of the attack and business impact. The Company conducted an extensive investigation to determine what unauthorized activity had occurred. At this time, the Company estimates the time frame of exposure of personally identifiable information to unauthorized actors to be October 21, 2020 to October 25, 2020.

Beginning on November 20, 2020, the Company sent letters via USPS First-Class mail to approximately 2,543 Washington residents notifying them that they may have been impacted by the ransomware attack. A sample copy of the notification letter is enclosed. While the Company to date has no confirmed evidence that any individual had their personal identification information misused, the Company chose to notify these individuals out of an abundance of caution so that they could take appropriate steps such as remaining vigilant, reviewing account statements, and monitoring credit reports.

The affected information that may have been accessed includes name, address, date of birth, phone number, Social Security number, email address, passport information, FMLA certification forms, and in certain limited circumstances, auto-deposit or other banking information. At this time, the Company is unable to determine precisely what personal information the unauthorized actor may have accessed, if at all.

Since the incident, the Company has taken proactive steps to mitigate risks and has increased its security measures designed specifically to protect its electronic systems and data. The Company is confident these additional measures will reduce the risk from similar cyber attacks.

Please do not hesitate to contact me if you have any questions or concerns regarding this matter.

Sincerely,

Emi A. Donis

Emi A. Donis
General Counsel, North America
Senior Operations LLC
(818) 531-5210
edonis@seniorplcusa.com

Enclosure: Sample notification letter to WA residents

November 20, 2020

Subject: Notification of Data Breach

Dear Recipient:

Senior Operations LLC is sending you this letter to provide you with information about an incident that may have resulted in the exposure of your personal information.

What Happened? In late October 2020, our systems were broadly hit with a ransomware attack. On October 24, 2020, we took action and shut down all of our systems to mitigate the extent of the attack and business impact. We also conducted an investigation and estimate the time frame of exposure to be October 21 to October 25, 2020. Our most recent investigation identified you as potentially impacted by the ransomware attack. While we have no confirmed evidence that you were impacted or that any individual had their personal identification information misused, we are notifying you out of an abundance of caution so that you may take appropriate steps such as remaining vigilant, reviewing account statements, and monitoring credit reports.

What Information Was Involved? Currently, we have no confirmation that any individual's personal identification information was specifically accessed or misused. The affected information that may have been accessed includes your name, address, date of birth, phone number, Social Security number, email address, and, if previously submitted to AMT/Damar, passport information and/or FMLA certification forms, and in certain limited circumstances, auto-deposit or other banking information. As stated above, we are unable to determine precisely what personal information the unauthorized actor may have accessed.

What We Are Doing. Since the incident, we have taken proactive steps to mitigate risks and have broadened as well as added depth to our security measures designed specifically to protect our systems and data. For security reasons, we cannot detail those activities here. However, we are confident these additional measures reduce the risk from similar cyber attacks.

What You Can Do. We urge you to be vigilant and follow the steps recommended on the attached page titled "Information About Identity Theft Protection" to further protect your personal information. You should also promptly report any fraudulent activity or suspected incident of identity theft to law enforcement authorities, the Washington Attorney General, and the Federal Trade Commission (FTC). In addition, you can obtain a copy of your credit report at no cost at www.annualcreditreport.com. See attached for more detail.

For More Information. We take your privacy very seriously and regret any inconvenience or concern this situation may cause. We hope this information is useful to you. If you have any questions, please do not hesitate to contact us by email at bkinser@amtnw.com or by phone at (360) 403-2024.

Sincerely,

Brady Fitzpatrick
VP/GM PNW
Senior Aerospace AMT and Damar

Information About Identity Theft Protection

Review your credit reports. We recommend that you remain vigilant by reviewing your personal 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 law enforcement, the attorney general and the FTC. To contact the Washington Attorney General, go to www.atg.wa.gov or call 1-800-551-4636. To file a complaint with the FTC, go to www.ftc.gov/idtheft or call 1-877-ID-THEFT (1-877-438-4338).

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. 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:

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
800.525.6285	888.397.3742	800.680.7289
P.O. Box 740256	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
equifax.com	experian.com/fraud	transunion.com/fraud

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.

Place a 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 may place a free security freeze on your credit report by contacting all three national credit reporting bureaus using the contact information below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting bureaus.

Equifax Security Freeze	Experian Security Freeze	TransUnion Security Freeze
800.685.1111	888.397.3742	888.909.8872
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
equifax.com	experian.com/freeze	transunion.com/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. In order to place the security freeze, you will need to supply your name, address, date of birth, Social Security number, and other personal information.

You can obtain additional information about the steps you can take to avoid identity theft from the Federal Trade Commission, which also encourages those who discover that their information has been misused to file a complaint with them. You can contact them at Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580, www.consumer.ftc.gov, 1-877-IDTHEFT (438-4338).