COHEN & GRESSER LLP

800 Third Avenue
New York, NY 10022
+1 212 957 7600 phone
www.cohengresser.com

Christian R. Everdell
212 707 7268
ceverdell@cohengresser.com

July 21, 2022

Via Email and Certified Mail

Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301
DOJ-CPB@doj.nh.gov

To Whom It May Concern:

We represent SHI International Corp. ("SHI") and write pursuant to N.H. Rev. Stat. Ann. § 359-C:20 to notify you of a data security incident at SHI that may have affected certain current and former SHI employees who reside in New Hampshire. By providing this notice, SHI does not waive any rights or defenses, nor does it consent to personal jurisdiction in New Hampshire.

On July 4, 2022, SHI discovered that an unauthorized party had gained access to its computer systems. The date of the initial access by the unauthorized party is still under investigation, but SHI currently believes that it may have occurred on or about June 28, 2022. SHI's security and IT teams swiftly identified the incident and measures were enacted to minimize the impact on SHI's employees and data. Although SHI was able to contain the incident, SHI believes that the unauthorized party obtained certain data, which may relate to approximately 15 current and former SHI employees who reside in New Hampshire.

While SHI's investigation into this incident is ongoing, SHI currently believes that the affected information pertains to only certain SHI employees. For those affected employees, the data could include one or more of the following categories of information: the employees' full names; social security numbers; home addresses; job titles; dates of employment and salary; tax, banking and loan information; or the employees' COVID-19 vaccination status and dates of any COVID-19 illness, to the extent reported to SHI.

SHI has notified federal law enforcement, including the FBI and the Cybersecurity and Infrastructure Security Agency, and is working closely with outside cybersecurity experts to thoroughly investigate the incident and restore SHI's systems to full availability in a secure and reliable manner. SHI is also implementing heightened security measures to further protect its information and the integrity of its systems and operations.

SHI is committed to protecting the privacy of personal information and safeguarding its employees from fraud and identity theft. As a courtesy, and in an abundance of caution, SHI has offered a complimentary two-year enrollment in a credit monitoring service to all of its current employees and will offer the same service to any former employees who may have been affected by the incident.

Enclosed for your reference is a copy of the notice that SHI intends to send to affected individuals on July 22, 2022, pursuant to N.H. Rev. Stat. Ann. § 359-C:20, which provides information on additional steps that current and former SHI employees can take to further protect their information.

We are available to discuss at your convenience.

Yours sincerely,

Christian R. Everdell

SHI International Corp.
290 Davidson Avenue
Somerset, NJ 08873
888-764-8888
SHI.com

July 22, 2022

NOTICE OF DATA BREACH

We are writing to provide you with information regarding a recent data security incident at SHI. The protection of your data is a matter we take very seriously and we recommend that you review the information in this letter for some steps you can take to protect yourself against potential misuse of your information.

What Happened?
On July 4, 2022, SHI discovered unauthorized access to its computer systems. SHI's security and IT teams swiftly identified the incident and measures were enacted to minimize the impact on SHI's systems and data. Although SHI was able to contain the incident, SHI believes that the unauthorized party may have obtained some data. While the number of individuals and the nature of the information affected is still being investigated, your data may have been among the compromised data.

What Information Was Involved?
While the investigation is still ongoing, SHI currently believes that the affected information does not pertain to all SHI employees. For those affected employees, the data could include one or more of the following categories of information: the employees' full names; social security numbers; home addresses; job titles; dates of employment and salary; tax, banking and loan information; or the employees' COVID-19 vaccination status and dates of any COVID-19 illness, to the extent reported to SHI.

What We Are Doing:
SHI is diligently investigating this matter and is working with the assistance of outside cybersecurity experts to further investigate the incident and restore SHI's systems to full availability in a secure and reliable manner. SHI's security and IT teams took some systems, including SHI's public websites and email, offline while the incident was being investigated and the integrity of those systems was assessed. SHI's systems and operations are steadily being restored and the forensic investigation is continuing together with the expert consultants. SHI is implementing heightened security measures to further protect your information and the integrity of our systems and operations.

In addition to conducting its own investigation, SHI is working with federal law enforcement including the FBI and the Cybersecurity and Infrastructure Security Agency.

Furthermore, to help safeguard your data, and to address any concerns you may have about this incident, we have arranged for complimentary enrollment, at your option, in **Equifax Complete Premier** credit monitoring service for two years. This service helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

- You already received information about Equifax Complete Premier in a previous email and may have already activated your monitoring service. If you have already done so, you do not have to activate it again.
- If you have not activated your monitoring service, you can find detailed instructions on how to activate your monitoring service in the hyperlink contained in the cover email.

What You Can Do:
Even if you do not wish to enroll in Equifax Complete Premier, it is important to remain vigilant by reviewing account statements and monitoring free credit reports for incidents of fraud and identity theft or errors. If you want extra security, you can take the following steps to further protect yourself:

- **Social Security Number Protections**: You have a right under the Fair Credit Reporting Act to place a fraud alert or security freeze on your credit files. A fraud alert requires potential creditors to use what the law refers to as "reasonable policies and procedures" to verify your identity before issuing credit in your name. The alert will remain on your accounts for 90 days. A security freeze will lock your credit files so nobody can access them to obtain credit in your name and is available free of charge. You can unlock them temporarily or permanently at any time.

  In order to request a security freeze, you will need to provide some or all of the following information to the credit reporting agency, depending on whether you do so online, by phone, or by mail:

  1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
  2. Social Security Number;
  3. Date of birth;
  4. If you have moved in the past five (5) years, the addresses where you have lived over the prior five years;
  5. Proof of current address, such as a current utility bill, telephone bill, rental agreement, or deed;
  6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
  7. Social Security Card, pay stub, or W2;
  8. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

  You can request a fraud alert or security freeze, which are free of charge, through any one of the three credit reporting agencies listed below. You can also request copies of your credit report from any of these agencies, which you should check for suspicious activity. If you find anything, contact the police or proper local authorities and file a report of identity theft. You have the right to obtain a copy of the police report. Ask for a copy of the police report, as you may need to supply this to your creditors.

  - Experian: P.O. Box 9554, Allen, TX 75013, www.experian.com, Phone: 888.397.3742

- Equifax: P.O. Box 740256, Atlanta, Georgia 30374, www.equifax.com, Phone: 800.525.6285
- TransUnion: P.O. Box 2000 Chester, PA 19016, 800-680-7289, www.transunion.com Phone: 800.680.7289.

You may obtain additional information on your rights under the Fair Credit Reporting Act from the Consumer Financial Protection Bureau at https://files.consumerfinance.gov/f/documents/bcfp_consumer-identity-theft-rights-summary_2018-09.docx.

- **Report Identity Theft**: Immediately report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding identity theft and information about fraud alerts and security freezes.

  - FTC: 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.identitytheft.gov

- **For residents of the District of Columbia**: You may obtain additional information on steps you can take to avoid identity theft from the Office of the Attorney General for the District of Columbia at (202) 727-3400; 400 6th Street, NW, Washington, DC 20001; or online at https://oag.dc.gov/consumer-protection.

- **For residents of Maryland**: You may obtain additional information on steps you can take to avoid identity theft from the Office of the Maryland Attorney General at 410-576-6300; 200 St. Paul Place, Baltimore, MD 21202; or online at https://www.marylandattorneygeneral.gov/Pages/CPD/.

- **For residents of New York**: You may obtain additional information on steps you can take to avoid identity theft from the New York Department of State Division of Consumer Protection at 1-800-771-7755 or https://dos.ny.gov/consumer-protection.

- **For residents of North Carolina**: You may obtain additional information on steps you can take to avoid identity theft from the Office of the North Carolina Attorney General at (919) 716-6400; 114 West Edenton Street, Raleigh, NC 27603; or online at https://ncdoj.gov/protecting-consumers/.

- **For residents of Rhode Island**: You may obtain additional information on steps you can take to avoid identity theft by contacting the Office of the Rhode Island Attorney General at (401) 274-4400 or https://riag.ri.gov/consumerprotection.

More Information:
If there is anything that SHI can do to assist you, please contact us toll free at (800) 443-1527 or via email at incident@shi.com.

Sincerely,

Kevin C. McCann
General Counsel