18657

[Date]

[First Name Last Name]
[Address]
[City, State Zip]

RE: Notification of Security Incident and Potential Access to Sensitive Information

Dear [First Name],

We at ChemStation International Inc. ("ChemStation", "we") take the security and protection of your information seriously. We are providing you this letter to make you aware of a security incident that may have resulted in the unauthorized disclosure or access to your company's or possibly your personal information. We are providing this notice out of an abundance of caution and in accordance with applicable laws to further share information with you so you can better protect yourself and your business.

What Happened

On November 6, 2020, ChemStation first became aware of an incident potentially involving the unauthorized access to a ChemStation employee's email account by an unauthorized individual from outside the company (the "Incident"). ChemStation immediately secured the account in question and commenced an investigation. ChemStation confirmed that an unauthorized individual gained access to one ChemStation email account and potentially viewed the contents of that account. The Incident occurred intermittently between the dates of September 30, 2020, and November 6, 2020. No other ChemStation systems were accessed during the Incident. While the investigation did not identify any removal of information from the account, ChemStation and its forensic team are unable to confirm that information in the email account was not viewed or accessed.

What Information Was Involved

Based on the investigation we don't have reason to believe the intruder necessarily accessed part or all of the email inbox. We only know that the viewing or removal of information was possible as a result of the unauthorized access. Such data may include, but is not necessarily limited to:

- first, middle, and last name;
- company name;
- telephone number;
- postal address; and
- personal or business credit card number.

What We Did and What We Are Doing

Upon learning of the Incident on November 6, 2020, ChemStation immediately secured the email account. ChemStation engaged legal counsel and a third-party forensic investigation firm to identify the scope of the Incident and assist with further securing the email system and data. ChemStation also consulted with law enforcement. Upon completion of the investigation by the forensic firm, ChemStation implemented any changes recommended by its forensics firm to further improve its existing information security policies and to safeguard systems against a recurrence of such an event.

Following the forensic investigation, ChemStation then conducted an extensive review of the employee email account's contents to determine if any personal or sensitive information could have been accessed or viewed by the intruder during the Incident. After an analysis of the entire email account, ChemStation confirmed some communications and documents contained sensitive information sent by individuals and companies. ChemStation has been working to properly identify the affected individuals or companies, the data involved, and provide notice accordingly. In addition to this notice, ChemStation is providing notice of the Incident to applicable state authorities as required under applicable state law.

What You Can Do

We recommend you review any activity on credit or payment cards or related bank accounts used to make payments to ChemStation to ensure all activity is valid. If you identify any suspicious activity or if you have concerns at all, we recommend you report such activity to your card issuer and replace your credit card as soon as possible. Should your personal information be involved in this Incident, please be aware that such risks the can sometimes include identity theft and financial fraud. Please be vigilant about monitoring your personally identifiable information, in particular your credit report information and financial accounts, to protect against fraudulent activity.

We sincerely regret this has transpired and any concerns it has caused for you or your company. If you have personal concerns about identity theft, you can contact local law enforcement and file a police report, as well as contact the Federal Trade Commission, your state attorney general or one of the credit bureaus for more information about how to protect your individual identity.

For More Information:

If you should have any concerns about identity theft, you can place a fraud alert, place a security freeze, or order a free credit report by contacting any of the following credit bureaus at one of the phone numbers listed below or visiting their respective websites. Please refer to each credit bureau's instructions when making any such requests.

Equifax
1-888-548-7878
P.O. Box 740256

Atlanta, GA 30348
www.equifax.com
Experian
1-888-397-3742
P.O. Box 4500
Allen, TX 75013
www.experian.com

Trans Union
1-888-909-8872
P.O. Box 2000
Chester, PA 19022
www.transunion.com

Security Freezes. You can place a security freeze with the credit bureaus free of charge. Under state law, a security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services.

Fraud Alerts. You can place a fraud alert with the credit bureaus free of charge. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. Call any one of the three major credit bureaus. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. The initial fraud alert stays on your credit report for one year. You can renew it after one year.

Credit Reports. You can request that all three credit reports be sent to you, free of charge, for your review. Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Thieves may hold stolen information to use at different times. Checking your credit reports periodically can help you spot problems and address them quickly.

The FTC provides more information about how to protect your identity at either https://www.ftc.gov/ or https://www.identitytheft.gov/. You may also find additional information on any applicable rights under the Fair Credit Reporting Act or you may contact the FTC.

Federal Trade Commission
1-202-326-2222
Bureau of Consumer Protection
600 Pennsylvania Avenue, NW
Washington, DC 20580

Again, we sincerely regret that this has occurred. If you have any additional questions, please call [ ].

Sincerely,

[ChemStation Official Name and Title]