AMPHASTAR PHARMACEUTICALS, INC.
11570 6th Street, Rancho Cucamonga, CA 91730 · Telephone: (909) 980-9484 · Fax: (909) 980-8296

VIA MAIL

August 28, 2020

Attorney General Gordon MacDonald
New Hampshire Department of Justice
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Breach

Dear Attorney General MacDonald:

Pursuant to N.H. Rev. Stat. § 359-C:19 *et seq.*, we are writing to notify you of data security incident involving five (5) New Hampshire residents.

Identification of Parties
Amphastar Pharmaceuticals, Inc. ("Amphastar"), including its subsidiary Armstrong Pharmaceuticals, Inc. based in Canton, Massachusetts, is a specialty pharmaceutical company that is engaged in the development, manufacture and marketing of generic and proprietary injectable, intranasal and inhalation drug products. As the parent company of Armstrong Pharmaceuticals, Inc., Amphastar maintained the personal information referenced in this letter. Amphastar is headquartered at 11570 6th Street, Rancho Cucamonga, California 91730.

Nature of the Security Incident
On July 24, 2020, Amphastar learned for the first time that some company data had been posted on the internet without authorization on July 21. Most of the information was legacy data (approximately 15 years old) and included social security numbers of employees, contractors and some shareholders. The information was in electronic form and was not encrypted. Amphastar is not aware of any resulting identity theft, fraud, or financial losses to any individuals.

Amphastar immediately investigated this posting to learn what happened with the assistance of a leading specialist routinely retained to assess and mitigate cybersecurity incidents. The posting was determined to be related to an earlier ransomware attack on May 2, 2020 that had been fully contained without any indication that data had been removed based on available records. No payment was or will be made to the criminals responsible for this malicious/criminal act. Amphastar was able to use backups and restore business continuity promptly in order to serve its role as an Essential Business in manufacturing and supplying pharmaceutical drugs during the COVID-19 pandemic. As law enforcement and others have reported, ransomware attacks have increased and have targeted the healthcare industry in the United States and around the world including during the global pandemic.[1]

[1] COVID-19 Email Phishing Against US Healthcare Providers, FBI Flash (April 21, 2020) (Alert Number MI-000122-MW), https://www.aha.org/system/files/media/file/2020/04/fbi-alert-tlp-white-covid-19-email-phishing-against-us-healthcare-providers-4-21-2020.pdf; *see also* Cybercriminals targeting critical healthcare institutions with ransomware, INTERPOL News and Events (April 4, 2020), https://www.interpol.int/en/News-and-Events/News/2020/Cybercriminals-

Other personal information was not involved. For example, Amphastar has confirmed that there was no driver's license number or state-issued identification card number, financial account number, or credit or debit card number. Amphastar does not maintained this personal information on its network.

Number of New Hampshire Residents Affected
Amphastar has determined that this incident affected five (5) individuals residing in New Hampshire whose personal information was the subject of the incident. This New Hampshire residents will shortly receive notice pursuant to N.H. Rev. Stat. § 359-C:19 *et seq.* by mail. While there is no evidence that the personal information was misused, Amphastar wanted to ensure that each individual received notice so they could be aware of this incident and take steps to protect themselves. A copy of the notice sent to these individuals is attached.

Response to the Incident
Once the incident was discovered, Amphastar immediately conducted an investigation. Amphastar responded quickly to the threat actor was removed. Amphastar has not reported this incident to law enforcement. There is insufficient information to identify the criminal actors responsible for this incident. There is no evidence that any of the personal information was used for fraudulent purposes. Amphastar is offering two years of credit monitoring services for all three credit bureaus to the affected individuals, free of charge, as outlined below.

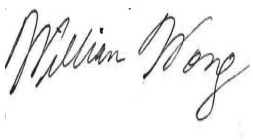
Credit Monitoring
The affected personal information includes social security numbers. Amphastar is providing the affected individuals, free of charge, 24 months of credit monitoring services through the Experian® IdentityWorks℠ which provides identity detection and resolution of identity theft protection for all three credit bureaus. The affected individuals have not been asked or required to waive any right of private action as a condition of accepting the credit monitoring services.

// // //

targeting-critical-healthcare-institutions-with-ransomware; Ryan Gallagher and Bloomberg, Hackers 'without conscience' demand ransom from dozens of hospitals and labs working on coronavirus, Fortune (April 1, 2020), https://fortune.com/2020/04/01/hackers-ransomware-hospitals-labs-coronavirus; High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations, FBI Public Service Announcement (Oct. 2, 2019) (Alert Number I-100219-PSA), https://www.ic3.gov/media/2019/191002.aspx.

Contact Information
If you have any questions concerning this matter, please contact me at (909) 980-9484.

Sincerely,



William Wong, Esq.
Acting General Counsel
Amphastar Pharmaceuticals, Inc.

Attachment

AMPHASTAR PHARMACEUTICALS, INC.
11570 6th Street, Rancho Cucamonga, CA 91730 · Telephone: (909) 980-9484 · Fax: (909) 980-8296

August 28, 2020

[Individual's Name]
[Individual's Address]

Re: Notice of Data Breach

Dear [Individual],

At Amphastar Pharmaceuticals, Inc., and its subsidiaries International Medication Systems, Ltd., and Armstrong Pharmaceuticals, Inc. (collectively, the "Company"), we take the privacy of our employees and former employees very seriously. It is important to us that you are made aware of an isolated security incident involving your personal information and to identify steps you can take to protect yourself. The Company has policies in place to protect confidential information including the personal information of its employees.

What Happened?

On July 24, 2020, the Company learned for the first time that some Company data had been posted on the internet without authorization on July 21. Most of the information was legacy data (approximately 15 years old) and included some of your personal information along with other company records.

The Company immediately investigated this posting to learn what happened with the assistance of a leading specialist routinely retained to assess and mitigate cybersecurity incidents. The posting was determined to be related to an earlier ransomware attack on May 2, 2020 that had been fully contained without any indication that data had been removed based on available records. No payment was or will be made to the criminals responsible for this malicious/criminal act. The Company was able to use backups and restore business continuity promptly. As law enforcement and others have reported, ransomware attacks have increased and have targeted the healthcare industry in the United States and around the world including during the global pandemic.[1]

What Information Was Involved?

The personal information that was involved included your first and last name and Social Security Number.

[1] COVID-19 Email Phishing Against US Healthcare Providers, FBI Flash (April 21, 2020) (Alert Number MI-000122-MW), https://www.aha.org/system/files/media/file/2020/04/fbi-alert-tlp-white-covid-19-email-phishing-against-us-healthcare-providers-4-21-2020.pdf; *see also* Cybercriminals targeting critical healthcare institutions with ransomware, INTERPOL News and Events (April 4, 2020), https://www.interpol.int/en/News-and-Events/News/2020/Cybercriminals-targeting-critical-healthcare-institutions-with-ransomware; Ryan Gallagher and Bloomberg, Hackers 'without conscience' demand ransom from dozens of hospitals and labs working on coronavirus, Fortune (April 1, 2020), https://fortune.com/2020/04/01/hackers-ransomware-hospitals-labs-coronavirus; High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations, FBI Public Service Announcement (Oct. 2, 2019) (Alert Number I-100219-
Social security number.
(2) Driver's license number or other government identification number.
(3) Account number, credit card number, or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.PSA), https://www.ic3.gov/media/2019/191002.aspx.

To be clear, other personal information was not involved. For example, the Company has concluded that there was no driver's license, or other government identification number; or account number, credit card number, or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account. Additionally, there was no medical or health insurance information, biometric data, or user name or email address along with a password or security question and answer.

What We Are Doing

We wanted to let you know this happened and assure you we take this matter very seriously. Once we became aware of this incident, we consulted with the leading specialist in the field, who confirmed that the situation has been contained and that the threat actor has been removed. There has been no further communication from the threat actor since the initial demand on May 2, 2020.

Although we have no evidence that your information was misused, we concluded that it is important to make you aware of this incident. We are also providing 24 months of fraud detection and identity restoration services through Experian, at no cost to you, as summarized in the attachment (How to Enroll in Credit Monitoring).

What You Can Do

We encourage you to consider these measures to monitor and protect your personal information and to remain vigilant for potential incidents of fraud and identity theft:

- **Vigilance**: Regularly monitor your financial accounts and, if you see any unfamiliar activity, promptly contact your financial institution. Monitor your credit reports, which are available free of charge, as noted below.

- **Free Annual Credit Report**: Obtain a free annual credit report from each of the three national consumer credit reporting companies (Experian, Equifax, and TransUnion) by calling (877) 322-8228 or by logging onto www.annualcreditreport.com.

- **Fraud Alert**: You may place a "fraud alert" on your credit file to ask creditors to contact you before they open any new accounts or change your existing accounts. This request, which can be made from any of the three national consumer credit reporting companies, can help detect any possible misuse of your personal information. Note that a fraud alert may protect you but also may cause delay when you seek to obtain credit. The initial fraud alert is active for 90 days and can be renewed.

- **Security Freeze**: You may place a "security freeze" on your credit files. A freeze prevents an authorized person from using your personal identifying information to open new accounts or borrow money in your name. You will need to contact the three national consumer credit reporting companies at the toll-free telephone numbers or websites listed below. The fee is $10 for each credit reporting agency, but the agencies may waive the fee if you can prove that identity theft has occurred. 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.

  // // //

Equifax	Experian	TransUnion
P.O. Box 105069	P.O. Box 4500	P.O. Box 105281
Atlanta, GA 30348	Allen, TX 75013	Atlanta, GA 30348
(800) 525-6285	(888) 397-3742	(800) 680-7289
www.equifax.com	www.experian.com	www.transunion.com

For additional security freeze information, from the North Carolina Attorney General's Office, visit: https://ncdoj.gov/protecting-consumers/protecting-your-identity/free-security-freeze/

- **Federal Trade Commission**: The FTC website has further information regarding preventing fraud and identity theft, including additional information about "fraud alerts" and "security freezes," and about how to monitor and protect your credit and finances. Additional information about preventing identify theft may also be obtained from:

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, D.C. 20580
(202) 326-2222
1-877-382-4357
www.consumer.ftc.gov/features/feature-0014-identity-theft
www.IdentityTheft.gov

- **Internal Revenue Service**: The Internal Revenue Service provides information in the event that tax-related identity theft may be suspected: https://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft. In addition, the Internal Revenue Service offers victim assistance at: https://www.irs.gov/individuals/how-irs-id-theft-victim-assistance-works

For More Information

We sincerely regret that this incident occurred. The Company is committed to protecting the privacy and security of personal information of those we do business with. For more information, please contact us at (909) 980-9484.

Sincerely,

Dan Dischner
Vice President of Corporate Communications and Human Resources
Amphastar Pharmaceuticals, Inc.

How to Enroll in Credit Monitoring

As noted, to help protect your identity, we are offering a complimentary two-year membership of Experian's® IdentityWorks℠. This product provides you with identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Name: [Individual]
- Ensure that you **enroll by**: **November 30, 2020** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: **https://www.experianidworks.com/3bcredit**
- Provide your **activation code**: **[code]**
- Provide engagement number **[number]**.

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at (877) 890-9332 by **November 30, 2020** Be prepared to provide engagement number **[number]** as proof of eligibility for the identity restoration services by Experian.

Additional Details Regarding Your 24-Month Experian Identityworks Membership:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.[1]
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™**: You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance:**[2] Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at [customer service number]. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

---

[1] Offline members will be eligible to call for additional reports quarterly after enrolling.

[2] The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.