US MED
United States Medical Supply

Return Mail Processing
PO Box 999
Suwanee, GA 30024

1 1 1 **********SNGLP
SAMPLE A. SAMPLE - L01
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

January 12, 2024

RE: Notice of Data Breach. Please read this entire letter.

Dear Sample A. Sample:

We are writing to inform you that United States Medical Supply ("US MED") suffered a security incident that may affect you. The security incident is described below along with steps you can take to protect yourself against identity theft and information on credit monitoring services provided to you by US MED at no charge.

Why are we contacting you?

The security incident may have resulted in unauthorized access to your personal information.

What Personal Information Was Involved?

During routine quality assurance checks of our customer service agents' telephone interactions with US MED customers, we discovered a breach of US MED protocols that resulted in the security incident. On November 13, 2023, a member of US MED's quality assurance team, conducting routine quality checks of telephone calls between US MED customers and US MED customer service agents, noted suspicious activity on a number of calls. Namely, it appeared that one US MED customer service agent allowed another individual that is not associated with US MED ("unauthorized individual") to conduct telephone conversations with US MED customers. US MED immediately severed the employee's access to US MED customer information, and the employee was terminated the following day. Over the next week, US MED conducted a thorough investigation of this security incident. On November 20, 2023, it was determined that the unauthorized individual may have had access to your name, phone number, date of birth, address, sensitive health information such as information related to your health diagnosis, and internal US MED patient ID number.

What Are We Doing.

In light of the incident, we are reviewing our security policies and procedures, our employee policy and procedures, our employee training procedures, and our work from home procedures. We are updating all our policies, procedures, and training based on our review to better protect against future occurrences. Additionally, we have flagged your patient ID's so that any activity related to you and any access to your information will only be handled by senior personnel.

What You Can Do.

We recommend that you stay vigilant with respect to your personal information and health records and notify us immediately at 1-844-638-2933 or at privacyofficer@northcoastmed.com, if there are any changes to your information that you did not authorize with respect to us. Additionally, to protect yourself from the possibility of identity theft, we recommend that you immediately place a fraud alert on your credit files. A fraud alert conveys a special message to anyone requesting your credit report that you suspect you may have been a victim of fraud. When you or someone else attempts to open a credit account in your name, the lender should take additional measures to verify that you have authorized the request. A fraud alert should not stop you from using your existing credit cards or other accounts, but it may slow down your ability to obtain new credit. An initial fraud alert is valid for ninety (90) days. To place a fraud alert on your credit reports, contact one of the three major credit reporting agencies at the applicable number listed below or via the agency's website. You only need to contact one agency, which will notify the other two on your behalf. You will then receive letters from the all agencies with instructions on how to obtain a free copy of your credit report from each.

Experian (888) 397-3742 or *www.experian.com* or
P.O. Box 2104, Allen, TX 75013

Equifax (888) 766-0008 or *https://www.equifax.com/* or
P.O. Box 740241, Atlanta, GA 30374

TransUnion (800) 680-7289 or *www.transunion.com* or
P.O. Box 2000, Chester, PA 19016

When you receive a credit report from each agency, review the reports carefully. Look for accounts you did not open, inquiries from creditors that you did not initiate, and confirm that your personal information, such as home address and Social Security number, is accurate. If you see anything you do not understand or recognize, call the credit reporting agency at the telephone number on the report. You should also call your local police department and file a report of identity theft. Get and keep a copy of the police report because you may need to give copies to creditors to clear up your records or to access transaction records.

Even if you do not find signs of fraud on your credit reports, we recommend that you remain vigilant in reviewing your financial account statements and future credit reports from the three major credit reporting agencies. You may obtain a free copy of your credit report once every 12 months by:

- visiting *www.annualcreditreport.com*,
- calling toll-free 877-322-8228, or
- completing an Annual Credit Request Form found at:
  w*ww.ftc.gov/bcp/menus/consumer/credit/rights.shtm* and mailing to:
  Annual Credit Report Request Service
  P.O. Box 1025281 Atlanta, GA 30348-5283

For more information on identity theft, you can visit the following Federal Trade Commission *website at: www.ftc.gov/bcp/edu/microsites/idtheft/*.

Additionally, if you received correspondence or any communication from the Internal Revenue Service that you may have been a victim of tax-related identity theft or that your tax filing was rejected as a duplicate, you should immediately fill out a Form 14039 Identity Theft Affidavit and submit it to the Internal Revenue Service. You should continue to file your tax return, as applicable, and attach the Form 14039 Identity Theft Affidavit to the return. Tax-related identity theft occurs when someone uses a taxpayer's stolen Social Security number to file a tax return claiming a fraudulent refund.

For more information on when to file a Form 14039 Identity Theft Affidavit, you can visit the following Internal Revenue Service website: *https://www.irs.gov/newsroom/when-to-file-an-identity-theft-affidavit*.

For more information on tax-related identity theft, you can visit the following Internal Revenue Service website: *https://www.irs.gov/newsroom/taxpayer-guide-to-identity-theft*.

You also have the right to put a Security Freeze on their credit reports. A Security Freeze prevents most potential creditors from viewing your credit reports and therefore, further restricts the opening of unauthorized accounts. It is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a Security Freeze may interfere with or delay your ability to apply for a new credit card, wireless phone, or any service that requires a credit check. A separate Security Freeze must be requested and placed on the applicable credit file with each credit reporting agency. To place a Security Freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, social security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement, or insurance statement. There is no charge to request a security freeze or to remove a Security Freeze.

To help protect your identity, we are offering complimentary access to Experian IdentityWorks^{SM} for 24 months. This will be separate from the fraud alert you may put on your credit files, as explained above.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. 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 from the date of the incident (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 with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for 24 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at *www.ExperianIDWorks.com/restoration*.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks^{SM} as a complimentary 24 month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you enroll by April 30, 2024 (Your code will not work after this date.)
- Visit the Experian IdentityWorksSM website to enroll: https://www.experianidworks.com/credit
- Provide your activation code: ABCDEFGHI

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks^{SM} online, please contact Experian's customer care team at 833-918-4493 by April 30, 2024. Be prepared to provide engagement number B112535as 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 IdentityWorksSM. 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.*
- Credit Monitoring: Actively monitors Experian file for indicators of fraud.
- Identity Restoration: Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- Experian IdentityWorks ExtendCARE^{TM}: You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- $1 Million Identity Theft Insurance**: Provides coverage for certain costs and unauthorized electronic fund transfers.

For More Information.

If there is anything that we can do to further assist you, please call, or email Maxo Joseph at 1-844-638-2933 or privacyofficer@northcoastmed.com.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** 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.

Additional State Specific Information

If you are a resident of Maryland:

- For more information on identity theft, you can visit or contact the Office of the Maryland Attorney General at the following:
  - Website: *https://www.marylandattorneygeneral.gov/*
  - Phone Number: 888-743-0023
  - Address: 200 St. Paul Place, Baltimore, MD 21202

If you are a resident of North Carolina:

- For more information on identity theft, you can visit or contact the Office of the North Carolina Attorney General at the following:
  - Website: *https://ncdoj.gov/protecting-consumers/protecting-your-identity/protect-your-business-from-id-theft/security-breach-information/*
  - Phone number: 919-716-6000
  - Address: 114 West Edenton Street, Raleigh, NC 27603

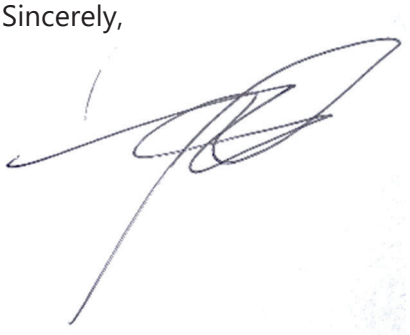
If you are a resident of New York:

- For more information on identity theft, you can visit the following websites or call the telephone number below:
  - New York Department of State Division of Consumer Protection at: *https://dos.ny.gov/consumer-protection*
  - NYS Attorney General at: *http://www.ag.ny.gov/home.html*
  - Phone Number: 800-771-7755

If you are a resident of Massachusetts:

- As a Massachusetts Resident, you also have the right to request and obtain a police report with regard to the cybersecurity attack.

Sincerely,



Maxo Joseph
Chief Compliance Officer