<<Date>> (Format: Month Day, Year)

<<b2b_text_3(Care of)>><<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Re: Data Security Incident

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

We are writing on behalf of Management and Network Services ("MNS") to inform you of an incident that may have involved some of your personal information. MNS provides some administrative support services to post-acute providers, and in connection with providing these services, MNS may receive information belonging to providers' patients. MNS may also receive information belonging to individuals who were referred to, but did not receive services from, a provider.<<b2b_text_1(ClientStatement)>> At MNS we take the privacy and security of personal information very seriously. This letter contains information about the incident and steps you can take to help protect your personal information.

What Happened? On or about August 21, 2019, we confirmed that several MNS employee email accounts may have been accessed without authorization at various times between April and July of 2019. Five (5) of the impacted email accounts were believed to contain personal or protected health information. In immediate response, we took steps to ensure the security of our email system and began analyzing the email accounts to determine what personal or protected health information may have been affected by the incident. The analysis recently revealed that some of your information was contained in the affected email accounts. We have no evidence to suggest that your personal information has been misused. Nonetheless, out of an abundance of caution, we are writing to inform you about the incident and to share with you steps you can take to help protect your personal information.

What Information Was Involved? The following information may have been involved in the incident: your <<b2b_text_2(ImpactedData)>>.

What We Are Doing. As soon as we discovered the incident, we took the steps described above. We also implemented additional security features for our email system to reduce the risk of a similar incident occurring in the future. In addition, though we are not aware of the misuse of any potentially impacted information, as a courtesy to you, we are offering you twelve (12) months of identity monitoring services at no cost to you through Kroll.

Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Web Watcher, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.idheadquarters.com** to activate and take advantage of your identity monitoring services.
*You have until **August 7, 2020** to activate your identity monitoring services.*
Membership Number: **<<Member ID>>**

Additional information describing your services is included with this letter.

What You Can Do. We encourage you to activate the services we are offering you, and to follow the recommendations

included with this letter. We also recommend that you review your credit report and consider placing a security freeze on your credit file. If you see anything that you do not understand or that looks suspicious, you should contact the three consumer reporting agencies listed under the section titled “Steps You Can Take to Further Help Protect Your Information” for assistance.

For more information: Further information about how to help protect your personal information appears on the following page. If you have questions, please call 1-866-377-0035, Monday through Friday from 9:00 a.m. to 6:30 p.m. Eastern Time, excluding major US holidays.

We take the privacy and security of personal information seriously, and we sincerely apologize for any worry or inconvenience that this incident may cause you.

Sincerely,

Jonathan E. Hoffman
Chief Executive Officer
Management and Network Services, LLC

Steps You Can Take to Further Help Protect Your Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com/, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print this form at https://www.annualcreditreport.com/cra/requestformfinal.pdf. You also can contact one of the following three national credit reporting agencies:

TransUnion
P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Experian
P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

Equifax
P.O. Box 105851
Atlanta, GA 30348
1-800-685-1111
www.equifax.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

Security Freeze: You have the right to put a security freeze on your credit file. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze 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 obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. There is no charge to place, lift or remove the security freeze. In order 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.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC or from your respective state Attorney General about steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state. Residents of Maryland, North Carolina, and Rhode Island can obtain more information from their Attorneys General using the contact information below.

Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

North Carolina Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General
150 South Main Street
Providence, RI 02903
http://www.riag.ri.gov
401-274-4400

You also have certain rights under the Fair Credit Reporting Act (FCRA), including: to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information, as well as others. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

Deceased Consumers: Upon the death of a consumer, the three major credit bureaus, Equifax, Experian and Trans Union, will flag a deceased consumer's credit file to prevent the credit file information from being used to open credit without authorization. To notify the three major credit bureaus that a consumer is deceased, you should mail a copy of the consumer's death certificate to:

Equifax
Equifax Information Services
P.O. Box 105169,
Atlanta, GA 30348

Experian
Experian Information Services
P.O. Box 9701
Allen, TX 75013

TransUnion
Trans Union Information Services
P.O. Box 2000
Chester, PA 19022

Kroll | A Division of DUFF & PHELPS

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services[1] from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

[1] Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.
To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.