WILSON ELSER

March 18, 2016

Gregory Bautista
914.872.7839 (direct)
Gregory.Bautista@wilsonelser.com

Attorney General Joseph Foster
Office of the Attorney General
33 Capitol Street
Concord, NH 03302

Dear Attorney General Foster:

We represent Management Health Systems, Inc. d/b/a MedPro Healthcare Staffing ("MHS"), a company that provides staffing services to healthcare facilities throughout the United States, with respect to a recent potential data security incident. MHS takes the security and privacy of the information in its control seriously, and has taken steps to prevent a similar incident from occurring in the future.

1. Nature of security incident.

On March 8, 2016, MHS discovered that an employee was the subject of a phishing attack when they received an email purporting to be from the CEO of the company, requesting copies of employee W-2 wage and tax statements. The employee responded to the request and sent electronic copies of the requested documents. MHS immediately began an investigation and determined that the request did not come from the CEO of the company, but from an unknown e-mail address that was made to appear to be the CEO. The W-2 forms sent contained employees' names, addresses, Social Security numbers, and certain income information for 2015. MHS notified law enforcement and the IRS of the incident and is continuing to cooperate with their investigation.

At this time MHS is not aware of any misuse of any employee information. However, out of an abundance of caution, MHS has notified the affected individuals and offered them free credit monitoring and identity protection services for 12 months at no cost to them.

2. Number of New Hampshire residents affected.

Six (6) New Hampshire residents were affected by the security incident. A notification letter to each individual was mailed on March 18, 2016 via regular mail. A copy of the notification letter is included with this letter.

3. Steps MHS have taken or plan to take relating to the incident.

MHS has taken steps to prevent a similar incident from occurring again. This includes additional training of employees, revising our policies and procedures regarding the handling of personal information, strengthening IT procedures to further block spoofing emails like the one used in this incident, and conducting a full network security audit to identify known malware. MHS is also offering potentially affected individuals with credit monitoring and identity protection services through AllClear ID.

4. Contact information.

MHS remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at Gregory.Bautista@wilsonelser.com or 914-872-7839.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

Gregory Bautista

Enclosure

2054330v.1

MANAGEMENT HEALTH SYSTEMS, INC.
d/b/a MEDPRO HEALTHCARE STAFFING

Processing Center • P.O. BOX 141578 • Austin, TX 78714

00025
JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

March 18, 2016

Dear John Sample:

We are writing to inform you of a data security incident that may have resulted in the disclosure of your personal information, including your name and Social Security number. We take the security of your personal information very seriously, and sincerely apologize for any inconvenience this may cause you. This letter contains information about steps you can take to protect your information, and resources we are making available to help you.

On March 8, 2016, we discovered that an employee was the subject of a phishing attack when they received an email purporting to be from the CEO of the company, requesting copies of employee W-2 wage and tax statements. The employee responded to the request and sent electronic copies of the requested documents. We immediately began an investigation and determined that the request did not come from the CEO of the company, but from an unknown e-mail address that was made to appear to be the CEO's email address. The W-2 forms sent contain your name, address, Social Security number, and certain income information for 2015. At this time we are not aware of any misuse of your information. However, out of an abundance of caution, we have notified law enforcement (FBI) and the IRS of the incident and will continue to cooperate with these organizations in any ongoing investigation.

We have also arranged with AllClear ID to provide identity protection and repair services to you for a period of 12 months, at no cost to you. The following identity protection services start on the date of this notice and can be used any time during the next 12 months.

AllClear SECURE: The team at AllClear ID is ready and standing by if you need identity repair assistance. This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-877-412-7152 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear PRO: This service offers additional layers of protection including credit monitoring and a $1 million identity theft insurance policy. To use the PRO service, you will need to enroll, either online at enroll.allclearid.com or by calling 1-877-412-7152. To receive this service at no charge to you, use the following redemption code: Redemption Code.

Please note: Additional steps may be required by you in order to activate phone alerts from AllClear ID.

Additional information regarding AllClear ID's services, and other important information regarding preventing identity theft, obtaining credit reports and credit freezes is attached.

We want to assure you that we have taken steps to prevent a similar event from occurring in the future, and to protect the privacy and security of your information. This includes additional training of employees, revising our policies and procedures regarding the handling of personal information, strengthening IT procedures to further block spoofing emails like the one used in this incident, and conducting a full network security audit to identify known malware.

We take the privacy and security of your information very seriously, and sincerely regret any concern or inconvenience this may cause you. Please know that the protection and security of your personal information is a top priority for us. Please call 1-877-412-7152, Monday through Saturday, 8:00 a.m. to 8:00 p.m. Central Time with any questions or concerns. (Closed on U.S. observed holidays).

Sincerely,

Frank Forbes
Chief Financial Officer,
Chief Information Officer

Additional Important Information

For residents of *Hawaii, Michigan, Missouri, Virginia, Vermont,* and *North Carolina*: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of *Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon,* and *West Virginia*:
It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report by contacting any one or more of the following national consumer reporting agencies:

Equifax
P.O. Box 70241
Atlanta, GA 30374
1-800-685-1111
www.equifax.com

Experian
P.O. Box 22104
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19022
1-800-888-4213
www.transunion.com

You may also obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of *Iowa*:
State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of *Oregon*:
State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission.

For residents of *Maryland, North Carolina,* and *Illinois*:
You can obtain information from the Maryland and North Carolina Offices of the Attorneys General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023
www.oag.state.md.us

North Carolina Office of the Attorney General
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
1-877-566-7226
www.ncdoj.com

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/bcp/edu/microsites/idtheft

For residents of *Massachusetts*:
It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

For residents of all states:
Fraud Alerts: You can place fraud alerts with the three credit bureaus at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three credit bureaus is below:
Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.
***Security* Freeze:** You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to send a request to each consumer reporting agency by certified mail, overnight mail, or regular stamped mail. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. The consumer reporting agency may charge a fee of up to $5.00 to place a freeze or lift or remove a freeze, but is free if you are a victim of identity theft or the spouse of a victim of identity theft, and you have submitted a valid police report relating to the identity theft incident to the consumer reporting agency. You may obtain a security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
www.equifax.com

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
http://www.experian.com/freeze

TransUnion (FVAD)
P.O. Box 2000
Chester, PA 19022
www.transunion.com

More information can also be obtained by contacting the Federal Trade Commission listed above.

02-03-2

AllClear Secure Terms of Use

If you become a victim of fraud using your personal information without authorization, AllClear ID will help recover your financial losses and restore your identity. Benefits include:

- 12 months of coverage with no enrollment required;
- No cost to you – ever. AllClear Secure is paid for by the participating Company.

Services Provided
If you suspect identity theft, simply call AllClear ID to file a claim. AllClear ID will provide appropriate and necessary remediation services ("Services") to help restore the compromised accounts and your identity to the state prior to the incident of fraud. Services are determined at the sole discretion of AllClear ID and are subject to the terms and conditions found on the AllClear ID website. AllClear Secure is not an insurance policy, and AllClear ID will not make payments or reimbursements to you for any financial loss, liabilities or expenses you incur.

Coverage Period
Service is automatically available to you with no enrollment required for 12 months from the date of the breach incident notification you received from Company (the "Coverage Period"). Fraud events that occurred prior to your Coverage Period are not covered by AllClear Secure services.

Eligibility Requirements
To be eligible for Services under AllClear Secure coverage, you must fully comply, without limitations, with your obligations under the terms herein, you must be a citizen or legal resident eighteen (18) years of age or older and have a valid U.S. Social Security number. Minors under eighteen (18) years of age may be eligible, but must be sponsored by a parent or guardian. The Services cover only you and your personal financial and medical accounts that are directly associated with your valid U.S. Social Security number, including but not limited to credit card, bank, or other financial accounts and/or medical accounts.

How to File a Claim
If you become a victim of fraud covered by the AllClear Secure services (an "Event"), you must:

- notify AllClear ID by calling 1.855.434.8077 to report the fraud prior to expiration of your Coverage Period;
- provide proof of eligibility for AllClear Secure by providing the redemption code on the notification letter you received from the sponsor Company;
- fully cooperate and be truthful with AllClear ID about the Event and agree to execute any documents AllClear ID may reasonably require; and
- fully cooperate with AllClear ID in any remediation process, including, but not limited to, providing AllClear ID with copies of all available investigation files or reports from any institution, including, but not limited to, credit institutions or law enforcement agencies, relating to the alleged theft.

Coverage Under AllClear Secure Does Not Apply to the Following:
Any expense, damage or loss:

- due to
  - any transactions on your financial accounts made by authorized users, even if acting without your knowledge, or
  - any act of theft, deceit, collusion, dishonesty or criminal act by you or any person acting in concert with you, or by any of your authorized representatives, whether acting alone or in collusion with you or others (collectively, your "Misrepresentation");
- incurred by you from an Event that did not occur during your coverage period; or
- in connection with an Event that you fail to report to AllClear ID prior to the expiration of your AllClear Secure coverage period.

Other Exclusions:

- AllClear ID will not pay or be obligated for any costs or expenses other than as described herein, including without limitation, fees of any service providers not retained by AllClear ID; AllClear ID reserves the right to investigate any asserted claim to determine its validity.
- AllClear ID is not an insurance company, and AllClear Secure is not an insurance policy; AllClear ID will not make payments or reimbursements to you for any loss or liability you may incur.
- AllClear ID is not a credit repair organization, is not a credit counseling service, and does not promise to help you improve your credit history or rating beyond resolving incidents of fraud.
- AllClear ID reserves the right to reasonably investigate any asserted claim to determine its validity. All recipients of Secure coverage are expected to protect their personal information in a reasonable way at all times. Accordingly, recipients will not deliberately or recklessly disclose or publish their Social Security number or any other personal information to those who would reasonably be expected to improperly use or disclose that Personal Information.

Opt-out Policy
If for any reason you wish to have your information removed from the eligibility database for AllClear Secure, please contact AllClear ID:

E-mail	Mail	Phone
support@allclearid.com	AllClear ID, Inc. 823 Congress Avenue Suite 300 Austin, Texas 78701	1.855.434.8077