

June 10, 2016

VIA EMAIL, WITH PHYSICAL COPY TO FOLLOW BY MAIL

Remedi SeniorCare
One Olympic Place
Suite 600
Towson, MD 21204

[Name of Individual]

[Address]

Re: NOTICE OF DATA BREACH

Dear [Name],

What Happened

On June 6, 2016, Remedi SeniorCare ("Remedi") became aware that, on May 16, 2016, a criminal impersonating a senior company official requested and received the personal information of a number of Remedi employees, including their Social Security numbers. We regret that your information may be among that affected.

What Information Was Involved

Information found in employee W-2 forms, including name; address; wage information; state, local, and federal income tax information; and Social Security number, was involved in this incident.

Protecting the security of employee information is a responsibility that we take very seriously at Remedi and we are engaging legal, data security and law enforcement resources to address the incident and strengthen our data protection safeguards.

What We Are Doing

Upon learning of the incident, we contacted law enforcement and will cooperate with them to investigate this illegal activity.

What You Can Do

To help protect you, Remedi has engaged AllClearID to provide you with identity protection services for 24 months at no cost to you. 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 [###.###.####] and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

We have also engaged AllClear ID to provide you with the following identity protection for 24 months at no cost to you:

AllClear PRO: This service offers credit monitoring, a \$1 million identity theft insurance policy, and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition. To use the PRO service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com or by phone by calling [###.###.####] using the following redemption code: **{RedemptionCode}**.

Please note: Additional steps may be required by you in order to activate your phone alerts and monitoring options.

Even if you choose not to enroll in the services, we recommend that you remain vigilant about your personal information by reviewing account statements you have with other companies and by checking your credit report from one or more of the national credit reporting companies periodically. Following such reviews, you should promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities.

Because your Social Security number was involved, we recommend that you place a fraud alert on your credit files. You may add a fraud alert to your credit report file to make it more difficult for someone to get credit in your name by requiring creditors to follow certain procedures. It may also delay your ability to obtain credit. To place a fraud alert on your file, contact one of the three nationwide credit reporting agencies; the first agency that processes your fraud alert will notify the others to do so as well. You may also add a security freeze to your credit report file to prohibit a credit reporting agency from releasing information from your credit report without your prior written authorization.

Equifax
800.525.6285
P.O. Box 740241
Atlanta, GA 30374
www.equifax.com

Experian
888.397.3742
P.O. Box 9532
Allen, TX 75013
www.experian.com

TransUnion
800.680.7289
Fraud Victim Assistance Division
P.O. Box 6790
Fullerton, CA 92834
www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report. In addition, you may request that the Internal Revenue Service mark your account to identify any questionable activity by submitting Form 14039, "Identity Theft Affidavit," for actual or potential identity theft victims. This form is available at <https://www.irs.gov/pub/irs-pdf/f14039.pdf>.

We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding identity theft.

Federal Trade Commission, Consumer Response Center

600 Pennsylvania Avenue, NW, Washington, DC 20580, 1.877.IDTHEFT (438.4338),
www.ftc.gov/idtheft

Residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General: 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.

Residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from the North Carolina Office of the Attorney General: North Carolina Attorney General's Office, 9001 Mail Service Center, Raleigh, NC 27699, 1.877.566.7226, www.ncdoj.com.

For More Information

If you have any questions, please contact [###.###.###].

Sincerely,

Kathleen Chagnon
Senior Vice President and General Counsel