Addus HomeCare

Providing Quality Healthcare Since 1979

April 15, 2016

«AddressBlock»

«GreetingLine»

I am writing to make you aware that on March 31, 2016 Addus HomeCare was the victim of a fraudulent scheme which appears to have resulted in the unauthorized acquisition of the personal information contained in your W2 form for the year ending December 31, 2015. This incident may impact not only your tax return and refund, but also the personal information contained in your W2 form, including your first and last name, home address, and social security number. Upon learning of this fraud, we contacted law enforcement, including the FBI and the IRS, and have been working with them ever since to investigate this incident further and catch the perpetrators. We are very sorry for any inconvenience caused by this unfortunate incident.

Recommended action by the IRS

We take very seriously the security of our employees' information, and want to make sure you have the information you need so that you can take steps to help protect your personal information. In particular, as it relates to your tax return and refund, the IRS recommends you take the following action immediately:

- If you have already filed your tax return, your tax exposure is limited, but you should continue to monitor your accounts to ensure a duplicate return is not filed.

- If you have not yet filed your tax return, file your federal income tax return for 2015 as soon as possible so as to protect any tax refund you may be owed.

- If you try to file your tax return and it is rejected as a duplicate, your return may have been compromised. If you find your tax return has been compromised, you will need to file a paper copy of your return with the IRS, along with Form 14039, an Identity Theft Affidavit. According to the IRS, you will still receive your tax refund (if you are entitled to a tax refund), but it just may take longer as the IRS will need to confirm that you are truly the correct person to receive the refund. For more information, see the enclosed IRS Pamphlet "Identity Theft Information for Taxpayers," or visit www.identitytheft.gov.

- You can call the IRS at 1-800-908-4490 for further information and instructions.

Free credit monitoring

To further assist you in protecting yourself from identity theft, we have arranged for you to receive 12 months of free identity protection through Experian's ProtectMyID Alert program. This membership includes identity theft resolution services, a free credit report, daily credit monitoring to detect suspicious activity, and a $1 million identity theft insurance policy, including coverage of unauthorized electronic fund transfers from your bank account. Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of Chartis, Inc. The description provided in this letter is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

To offer added protection, you will receive ExtendCARE, which will provide you with fraud resolution support even after your ProtectMyID membership has expired. **Again, this protection is being offered at no cost to you.** You can register for these services by visiting the ProtectMyID Web Site: www.protectmyid.com/alert or calling (877) 297-7780 and providing the following activation code: **«Credit_Monitoring_Code»**. You have until **July 31, 2016** to register. If you have questions or need an alternative to enrolling online, please call (877) 297-7780 and provide Engagement # **PC100870**. Enrollment in ProtectMyID membership does not affect your credit score.

What are some further steps you can take to help protect yourself from identity theft?
We encourage you to remain vigilant for instances of fraud and identity theft. You should regularly review and monitor relevant account statements and credit reports to ensure the information contained in them is accurate. If you detect any unauthorized charges on your credit or debit card(s) you can contact your card issuer. If you see anything on your credit reports that is incorrect, contact the credit reporting agency. You should report suspected incidents of identity theft to local law enforcement, your Attorney General, or the Federal Trade Commission (the "FTC"). Even if you do not find any signs of fraud on your reports or account statements, the FTC and other security experts suggest that you check your credit reports and account statements periodically. We have included more information on these steps—and how to reach these entities—at the end of this letter.

Once again, we sincerely apologize for any inconvenience caused by this incident. If you have any questions about this notice or this incident or require further assistance, you can contact Jameson Eisenmenger at jeisenmenger@addus.com or 630-296-3461.

Sincerely,

Jameson Eisenmenger

Jameson Eisenmenger
Senior Vice President and General Counsel

Further Cautionary Steps to Protect Against Identity Theft

You can place a fraud alert.
You may elect to place a fraud alert with the major credit reporting agencies on your credit files. Their contact information is as follows:

Equifax	Equifax Information Services LLC P.O. Box 105069 Atlanta, GA 30348-5069	800-525-6285	www.equifax.com
Experian	Experian Fraud Reporting P.O. Box 9554 Allen, Texas 75013	888-397-3742	www.experian.com
TransUnion	TransUnion LLC P.O. Box 6790 Fullerton, California 92834-6790	800-680-7289	www.transunion.com

A fraud alert lasts 90 days, and requires potential creditors to use "reasonable policies and procedures" to verify your identity before issuing credit in your name (as soon as one agency is notified, the others are notified to place fraud alerts as well). When you contact these agencies, you can also request that they provide a copy of your credit report. You can keep the fraud alert in place at the credit reporting agencies by calling again after 90 days.

You can place a security freeze.
You can also ask these same credit reporting agencies to place a security freeze on your credit report. A security freeze prohibits a credit reporting agency from releasing any information from your credit report without your written authorization. Placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make. This may include requests for new loans, credit mortgages, employment, housing or other services. If you want to have a security freeze placed on your account, you must make a request in writing by certified mail to the reporting agencies. The reporting agencies will ask you for certain information about yourself. This will vary depending on where you live and the credit reporting agency. It normally includes your name, social security number, date of birth, and current and prior addresses (and proof thereof), and a copy of government-issued identification.

The cost to place, temporarily lift, or permanently lift a credit freeze varies by state. Generally, the credit reporting agencies will charge $5.00 or $10.00. However, if you are the victim of identity theft who has submitted a copy of a valid investigative or incident report, or complaint with a law enforcement agency, in many states it is free. You have the right to a police report under certain state laws.

Where else can you find information about how to avoid identity theft?
The FTC, your Attorney General, and the major credit reporting agencies listed above can provide additional information on how to avoid identity theft, how to place a fraud alert, and how to place a security freeze on your credit report. You can contact the FTC on its toll-free Identity Theft helpline: 1-877-438-4338. The FTC's website is http://www.ftc.gov/idtheft. Its address is Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Identity Theft Information for Taxpayers

Identity theft places a burden on its victims and presents a challenge to many businesses, organizations and governments, including the IRS. The IRS combats this crime with an aggressive strategy of prevention, detection and victim assistance.

What is tax-related identity theft?

Tax-related identity theft occurs when someone uses your stolen Social Security number (SSN) to file a tax return claiming a fraudulent refund. If you become a victim, we are committed to resolving your case as quickly as possible.

You may be unaware that this has happened until you e-file your return and discover that a return already has been filed using your SSN. Or, the IRS may send you a letter saying it has identified a suspicious return using your SSN.

Know the warning signs

Be alert to possible tax-related identity theft if you are contacted by the IRS about:

- More than one tax return was filed for you,
- You owe additional tax, have a refund offset or have had collection actions taken against you for a year you did not file a tax return, or
- IRS records indicate you received wages or other income from an employer for whom you did not work.

Steps for victims of identity theft

If you are a victim of identity theft, the Federal Trade Commission recommends these steps:

- File a complaint with the FTC at identitytheft.gov.
- Contact one of the three major credit bureaus to place a 'fraud alert' on your credit records:
  - www.Equifax.com 1-888-766-0008
  - www.Experian.com 1-888-397-3742
  - www.TransUnion.com 1-800-680-7289
- Close any financial or credit accounts opened by identity thieves

If your SSN is compromised and you know or suspect you are a victim of tax-related identity theft, the IRS recommends these additional steps:

- Respond immediately to any IRS notice; call the number provided or, if instructed, go to IDVerify.irs.gov.
- Complete IRS Form 14039, *Identity Theft Affidavit*, if your e-file return rejects because of a duplicate filing under your SSN or you are instructed to do so. Use a fillable form at IRS.gov, print, then attach form to your paper return and mail according to instructions.
- Continue to pay your taxes and file your tax return, even if you must do so by paper.
- If you previously contacted the IRS and did not have a resolution, contact us for specialized assistance at 1-800-908-4490. We have teams available to assist.

More information is available at: IRS.gov/identitytheft or FTC's identitytheft.gov.

About data breaches and your taxes

Not all data breaches or computer hacks result in tax-related identity theft. It's important to know what type of personal information was stolen.

If you've been a victim of a data breach, keep in touch with the company to learn what it is doing to protect you and follow the "Steps for victims of identity theft." Data breach victims should submit a Form 14039, *Identity Theft Affidavit,* only if your Social Security number has been compromised and IRS has informed you that you may be a victim of tax-related identity theft or your e-file return was rejected as a duplicate.

How you can reduce your risk

Join efforts by the IRS, states and tax industry to protect your data. Taxes. Security. Together. We all have a role to play. Here's how you can help:

- Always use security software with firewall and anti-virus protections. Use strong passwords.
- Learn to recognize and avoid phishing emails, threatening calls and texts from thieves posing as legitimate organizations such as your bank, credit card companies and even the IRS.
- Do not click on links or download attachments from unknown or suspicious emails.
- Protect your personal data. Don't routinely carry your Social Security card, and make sure your tax records are secure.

See Publication 4524, *Security Awareness for Taxpayers* to learn more.

NOTE: The IRS does not initiate contact with taxpayers by email to request personal or financial information. This includes any type of electronic communication, such as text messages and social media channels.