Willis

Website: www.willisbenefits.com
Phone: 800-231-1897
E-mail: Benefits_HR@willis.com

April 19, 2014

<Employee Name
Address
City, State Zip Code>

Dear Associate:

We previously notified you of the regrettable security incident recently experienced by the Willis North America Inc. Medical Expense Benefit Plan, which involved the accidental disclosure of some of your personal information. At the outset, we want to assure you that this letter has not been prompted by any developments since our last communication and that we have no reason to believe that any of the information has been misused. Rather, this letter provides you with legally required formal notice of that same incident, and includes some additional information, including additional steps you can take to help protect your identity.

What Happened?

On March 19, 2014, an email was sent internally to a group of current Willis Associates who were enrolled in the medical Plan's Healthy Rewards Program. The purpose of the email was to remind them of the upcoming deadline to earn wellness credits. Unfortunately, the person sending the reminder email accidentally attached a spreadsheet to the email that was not meant to be included. The spreadsheet contained the following information:

- Your name, Willis email address, date of birth, social security number, employee ID number, and office location by city/state/zip;
- Number of your Wellness credits and your credit status code, and insurance coverage codes for you (indicating whether coverage was for employee or for employee plus someone else (e.g., children, spouse or family));
- Internal codes for plan geographic region and type applicable to you (e.g., Healthy Rewards Plan; Healthy Savings Plan or Traditional Plan); and
- Dates (last effective date of your medical plan election or of election selection, your original and last start dates, and when medical plan coverage began for you).

The codes used were for internal administrative purposes only. The spreadsheet did **not** include any information that in any way revealed any of your health conditions, health treatments or health claims and did **not** include any personal information of your spouse or dependents.

The error was reported to us within minutes, and we took immediate and extensive remedial action to try to avoid any misuse of your information, including tracking and ensuring the deletion of any forwards of the email, blocking the ability to forward the email, and deleting the email from recipient inboxes. We instructed all recipients of the spreadsheet to delete any remaining copies, not to save or forward copies, and to report any misuse. We also completed an internal review of how this inadvertent error occurred and have

already begun implementing changes designed to prevent recurrence. As we described in our email to you of March 21, we have also arranged for you to receive identity theft protection for two years at no charge to you. In short, we have devoted extensive resources in an effort to avoid misuse of the information in the spreadsheet and to tighten procedures to help prevent such an incident in the future.

We have determined that this incident was not the result of an intentional or criminal act. Rather, it was the result of an unfortunate and regrettable, but entirely honest, mistake. Further, our current investigation leads us to believe that no improper use of the spreadsheet has occurred and that all copies of the spreadsheet have been deleted. Still, we continue to be diligent and our review of security procedures is ongoing. We ask for your continued diligence as well: this incident is an important reminder of the duty of all employees to maintain the confidentiality of sensitive information.

How to Register for Identity Theft Protection

As you will recall from our email to you of March 21, we have arranged for you to receive at no charge to you, two years of identity theft protection through the IDEssentials service offered by TrustedID, a subsidiary of Equifax and a leading provider of identity theft solutions. Details about the IDEssentials service can be found at www.trustedid.com/enhanced-identity-theft-protection (you may also wish to view TrustedID's applicable service terms of use and privacy policy). To register for the IDEssentials service online, go to **www.trustedid.com/willis** and **enter activation code WNAIDE0314**. You can also sign up by telephone, from 7 AM to 8 PM Central Time, 7 days a week at 1-888-880-0761. Identity theft specialists are available at this number to answer questions regarding these services. If you are already enrolled in an ID Theft Protection plan with TrustedID, you may have to use a different email address to enroll now, or contact TrustedID Customer Service at 1-888-880-0761 for assistance.

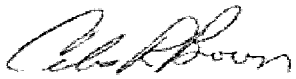
Additional Steps You Can Take

The attached Exhibit A includes contact information for the FTC and the major consumer reporting agencies as well as other disclosures and recommendations. The FTC's website provides information about a variety of protective measures, including how to obtain and review a free copy of your credit report, file a "fraud alert," request a "security freeze," file an identity theft report, watch for signs of identity theft generally, and decide whether to apply for a new social security number.

Should you have any questions regarding this letter, you can call Willis Benefits at 1-800-231-1897 or email us at benefits_hr@willis.com. Alternatively, you can contact the Willis Benefits Department at the following address: Willis North America Inc. Medical Expense Benefit Plan; Attention: Lynn Bissinger, Director, US Benefits; 26 Century Blvd.; Nashville, TN 37214.

Please accept our deepest apologies for this situation. We are reviewing and strengthening our data security practices in light of it and strongly encourage you to take the preventive measures outlined in this letter to help prevent, detect and report any misuse of the information.

Sincerely,



Celia Brown
Executive Vice President, Group Human Resources Director,
on behalf of the Willis North America Inc. Medical Expense Benefit Plan

Exhibit A
IDENTITY THEFT PREVENTION INFORMATION & U.S. STATE DISCLOSURES

The Federal Trade Commission as a Resource: The FTC provides guidance to help you deter, detect and defend against identity theft. You also may report suspected identity theft to the FTC.

***Obtain Free Credit Reports*:** We recommend that you check your credit report regularly. Each of the three credit reporting agencies must provide you annually with a free credit report, at your request made to a single, centralized source for the reports, www.annualcreditreport.com, the only Web site authorized by three agencies. That website also provides instructions for making a request by phone (1-877-322-8228) or by mail using a form supplied at the site and sent to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You are not required to order all three reports at the same time; instead, you may rotate your requests so that you can review your credit report on a regular basis. In addition, many states (*e.g.*, Iowa, Maryland, Michigan, Missouri, North Carolina, Oregon, Vermont and West Virginia) have laws that require these agencies to provide you with a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account.

Monitor Credit Reports, Monitoring Alerts and Accounts: When you receive credit reports, monitoring alerts and account statements, look for signs of fraud or identity theft and remain vigilant incidents of fraud or identity theft, including unauthorized activity. For example, look for accounts you did not open and personal information that you do not recognize, such as a home address or account numbers. If you have concerns, call the provider of the report or the account. You may also call your local police or sheriff's office to see if you may file a police report of identity theft and to obtain a copy of the police report. In Massachusetts, you have a right to obtain a police report if you are a victim of identity theft. Potentially, you may need to give copies of the police report to creditors to clear up your records.

Fraud Alerts and Security (or Credit) Freezes: According to the FTC, if you are a victim of identity theft and have created an Identity Theft Report, you may want to place an extended fraud alert or a credit freeze on your credit file. There are important differences between these two options:

- A freeze generally stops all access to your credit report, while a fraud alert permits creditors to get your report as long as they take steps to verify your identity.
- The availability of a credit freeze depends on state law or a consumer reporting company's policies; fraud alerts are federal rights intended for people who believe they are, or who actually have been, identity theft victims.
- Some states charge a fee for placing or removing a credit freeze, but it's free to place or remove a fraud alert

You can learn more about each of these options by visiting http://www.consumer.ftc.gov/articles/0279-extended-fraud-alerts-and-credit-freezes

Monitor Social Security Administration (SSA) Annual Statement of Benefits: When you receive your annual statement of benefits from the SSA, verify that the earnings reported to your social security number are accurate. The annual statement of benefits shows you all of the earnings reported using your social security number so if the wages reported there are greater than on your W2 form, you will know that there could be an employment identity theft problem. You may also check your reported earnings more frequently online by setting up an account with the SSA at http://www.ssa.gov.

***For residents of Hawaii, Michigan, Missouri, Vermont, Virginia*:** Hawaii Missouri, Vermont, and Virginia state laws advise you to remain vigilant by reviewing account statements and monitoring free credit reports; Michigan advises you to remain vigilant for incidents of fraud and identity theft .

***For residents of Iowa, Oregon, Maryland, and North Carolina*:** Iowa state law advises you to report any suspected identity theft to law enforcement or to the state's Attorney General at: Office of the Attorney General, 1305 E. Walnut Street, Des Moines, IA 50319 (515) 281-5164 www.iowaattorneygeneral.gov. Oregon state law advises you to report suspected identity theft to law enforcement and the Federal Trade Commission. North Carolina state law advises you to remain vigilant by reviewing account statements and monitoring free credit reports. The Maryland and North Carolina Offices of the Attorneys General will provide you with information about the steps you can take towards 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

For residents of West Virginia and Massachusetts: We are required to advise you that you have the right to place a security freeze on your consumer (credit) report. A freeze is designed to prevent credit, loans, and services from being approved in your name without your consent; however, using a freeze may delay your ability to obtain credit. Typically you may request that a freeze be placed on your consumer report by sending a request, along with proof of your identity, to each credit reporting agency by certified or overnight or regular stamped mail to an address designated by the credit reporting agencies, or by other lawful methods. Specifically, the following information should be included when requesting a freeze (documentation for you and your spouse must be submitted when freezing a spouse's consumer report): full name, with middle initial and any suffixes; Social Security number; date of birth (month, day and year); current address and previous addresses for the past two years; and applicable fee (if any) or incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request also should include a copy of a government issued ID card, such as a driver's license, state or military ID card, and a copy of a utility bill, bank or insurance statement. Each copy should be legible, display your name and current mailing address, and the date of issue (statement dates must be recent). The consumer reporting agency may charge a reasonable fee of up to $5.00 to place a freeze or lift or remove a freeze, unless you are a victim of identity theft or the spouse of a victim of identity theft, and have submitted a valid police report relating to the identity theft to the consumer reporting agency. Massachusetts residents have the right to obtain a police report if they are the victim of identity theft. Visit the websites or contact the credit reporting agencies for more information about placing a freeze, as they may have different requirements depending on the state in which you reside.

Contact Information for the FTC and the Consumer Reporting Agencies:

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/

AnnualCreditReport.com
Annual Credit Report Request Service
P.O. Box 105281
Atlanta, GA 30348-5281
www.annualcreditreport.com

Equifax
P.O. Box 740241
Atlanta, GA 30374
1-800-685-1111
www.equifax.com

Experian
P.O. Box 2104
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