



Notice of Data Breach

\_\_\_\_\_, 2016

(Participant Name)  
(Participant Address)

Dear \_\_\_\_\_,

We are writing to notify you of an incident that occurred on or around July 2016 that involved the potential, unauthorized access to your personal information.

**What Happened?** The unauthorized access was to a specific group of Irvine Company employees' personal information within the Core Benefit Administration (CBA) web portal (known to you as BenefitsNow) set up and maintained by Aon Hewitt, a benefits service provider. An unauthorized individual potentially accessed your personal information. We have confirmation that the unauthorized individual accessed 55 records of the 2,892 current or former employees receiving this letter. Since we cannot verify the identity of those 55 impacted employees, we are notifying you at this time of the unlikely, but potential access of your personal information. We sincerely apologize for any inconvenience you might experience as a result of this incident.

**What Information Was Involved?** The personal information potentially accessed by the unknown third person or persons was limited to your first and last name, social security number, saved contact information (such as mailing address or phone numbers), date of birth, beneficiary information, employee ID number, employment status, and health care plan status. The accessed data did not include any other personal information.

**What Are We Doing?** We have taken immediate steps to secure your personal information and to prevent this incident from recurring. Aon Hewitt is aware of the increasing threat of cybersecurity and phishing attacks on corporations and individuals. We employ rigorous security controls to protect personal data, including the personal data of Irvine Company's employees. Aon Hewitt is committed to making sure that we have security measures in place and effective training for our colleagues in order to help prevent such attacks from happening.

In addition, as a precaution, we are offering a **complimentary** one-year membership of InfoArmor's identity protection services. This product helps detect possible misuse of your personal information and provides you with superior identity protection services focused on immediate identification and resolution of identity theft. Please click on the link below to activate your credit monitoring membership:

#####

[www.infoarmor.com/protection](http://www.infoarmor.com/protection)



**What You Can Do?** Some easy steps you can take to safeguard your personal information include avoiding calls or emails from unknown sources that solicit your personal information, and using trusted security software that is set to update automatically. You should also remain vigilant by reviewing account statements and monitoring free credit reports. We have included some additional information to help in this regard appended to this letter. For more information on best practices visit [www.onguardonline.gov](http://www.onguardonline.gov). You should also report suspected incidents of any actual identity theft or fraud to local law enforcement, the Attorney General of the State of California and the FTC.

**For More Information.** If you have questions or wish to seek additional information, please contact the Irvine Company Benefits Service Center at 800-964-8570, Monday through Friday, 5 am to 5 pm Pacific Time.

Aon Hewitt takes the protection of your personal data very seriously, and we are committed to fully protecting all of the information entrusted to us. We appreciate your understanding of this matter, and we again apologize for any inconvenience.

Sincerely,

Aon Hewitt

Proprietary & Confidential



## **ADDITIONAL ACTIONS TO HELP REDUCE YOUR CHANCES OF IDENTITY THEFT**

### ➤ **PLACE A 90-DAY FRAUD ALERT ON YOUR CREDIT FILE**

An **initial 90 day security alert** indicates to anyone requesting your credit file that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the lender should take steps to verify that you have authorized the request. If the creditor cannot verify this, the request should not be satisfied. You may contact one of the credit reporting companies below for assistance.

**Equifax**  
1-800-525-6285  
[www.equifax.com](http://www.equifax.com)

**Experian**  
1-888-397-3742  
[www.experian.com](http://www.experian.com)

**TransUnion**  
1-800-680-7289  
[www.transunion.com](http://www.transunion.com)

### ➤ **PLACE A SECURITY FREEZE ON YOUR CREDIT FILE**

If you are very concerned about becoming a victim of fraud or identity theft, a security freeze might be right for you. Placing a freeze on your credit report will prevent lenders and others from accessing your credit report entirely, which will prevent them from extending credit. With a Security Freeze in place, you will be required to take special steps when you wish to apply for any type of credit. This process is also completed through each of the credit reporting companies.

### ➤ **ORDER YOUR FREE ANNUAL CREDIT REPORTS**

Visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call 877-322-8228. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

### ➤ **MANAGE YOUR PERSONAL INFORMATION**

Take steps such as: carrying only essential documents with you; being aware of whom you are sharing your personal information with and shredding receipts, statements, and other sensitive information.

### ➤ **USE TOOLS FROM CREDIT PROVIDERS**

Carefully review your credit reports and bank, credit card and other account statements. Be proactive and create alerts on credit cards and bank accounts to notify you of activity. If you discover unauthorized or suspicious activity on your credit report or by any other means, file an identity theft report with your local police and contact a credit reporting company.