July 18, 2017

[redacted]

[redacted]@sunbeltrentals.com

Re: Notice of Data Breach: Update on Recent "Phishing" Email Attack and Username and Password Compromise

Dear [redacted],

I am writing to follow-up on the telephone call that you received regarding an email phishing campaign that led to an unauthorized access to your Workday account. We wanted to provide you with more information about the nature of the campaign, as well as the steps we are taking and that you can take to better protect against the potential misuse of your information.

What Happened?

The fraudulent "phishing" email, which was sent by an unknown actor on June 12, 2017 pretending to be Kirby Miner, was designed to gain access to employees' user names and passwords. This email instructed the recipient to open an attachment and to enter their Sunbelt username and password. The link in the email's attachment then connected employees with an external phishing website. Once the credentials were entered by the employee, the bad actors then had the necessary information to sign-in to Sunbelt's company network, and to allow them access to certain services hosted by Workday. From the information we have gathered, it appears that the bad actors likely accessed your Workday account for a brief period of time.

What Employee Information Was Involved?

By accessing Workday, it is possible, but not yet determined, that the bad actors may have viewed sensitive personal information, including your name, address, e-mail address, company user name and password, social security number, payroll information, and limited information regarding any dependents and beneficiaries that are currently listed in Workday, but not the dependents' and beneficiaries' social security numbers. We are working with Workday as they continue to perform their own investigation of what exactly happened and what may have been visible to the bad actors. We can confirm that Sunbelt's IT Department detected the attack in time to prevent the bad actors from re-routing your paycheck, which we believe was their objective.

What Is Being Done About It?

Upon learning of the unauthorized access to our employees' Workday accounts, Sunbelt's IT personnel immediately implemented measures blocking the bad actor's IP address from accessing Workday accounts. By June 13th, the IT Department had also ensured that all recipients of the fraudulent email had reset their network passwords, thereby preventing any further access to the Sunbelt network or to Workday accounts. Since this phishing scam, Sunbelt has also invested in

enhanced security software and implemented additional security features within existing software that will assist in preventing similar attacks going forward.

What Is Being Done To Protect Me?

Securing your personal information is important to us. As a precautionary measure to safeguard your information from potential misuse, we have partnered with Equifax to provide its ID Patrol identity theft protection product to all affected employees for two years at no charge to you. A description of this product is provided in the attached material, which also contains instructions about how to enroll (including the personal activation codes). The activation code is unique and will only work for one individual.

If you choose to take advantage of the ID Patrol product, it will provide you with notification of any changes to your credit information, $1 million Identity Theft Insurance Coverage, access to your credit report, and Identity Restoration. If you become a victim of identity theft, an Equifax identity restoration specialist will work on your behalf to help restore your identity. We are also providing access to Equifax Identity Restoration if you become victim of identity theft by calling the number listed in your member center after you enroll.

You must complete the enrollment process by October 31, 2017. We urge you to consider enrolling in these products, at Sunbelt's expense, and reviewing the additional resources enclosed with this letter.

What Else Can I Do About It?

In addition to the free services provided by Sunbelt and Equifax, it is important for you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports and explanation of benefits forms for suspicious activity. You will have unlimited access to your Equifax Credit Report using the free activation codes attached.

Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com, call, toll free, 1-877-322-8228 or contact one of the three major credit bureaus directly to request a free copy of your credit report. At no charge, the major credit bureaus and the Federal Trade Commission ("FTC") can assist you regarding establishing a fraud alert on your credit file, preventing identity theft, or placing a security freeze on your credit reports. Should you wish to place a fraud alert, or should you have questions regarding your credit report, you can directly contact any of the three major credit reporting agencies and the FTC listed on the attached material.

We sincerely apologize for this incident. Please know that Sunbelt's investigation of this security incident is ongoing and we are continuously evaluating our processes and procedures to improve the security and safe handling of your information.

Who Can I Contact For More Information?

If you have questions about the Equifax credit monitoring and identity theft protection services or need assistance with fraud or identity theft issues, please call Equifax at (866) 820-9010.

If you have any additional questions, please feel free to contact the HR Hotline at 866-573-6246.

Sincerely,

Cheryl Black
SVP of HR

Kirby Miner
SVP of IT

Unique Activation Code for You in Workday:

First Name:	Middle Name:	Last Name:	Activation Code:
[redacted]			

EQUIFAX®

Equifax ID Patrol® Features and Enrollment Instructions

Equifax ID Patrol® provides you with the following key features:

- 3-Bureau credit file monitoring[1] and alerts of key changes to your Equifax®, TransUnion® and Experian® credit reports
- Access to your Equifax credit report
- One Equifax 3-Bureau credit report
- Wireless alerts (available online only). Data charges may apply.
- Automatic Fraud Alerts[2]. With a fraud alert, potential lenders are encouraged to take extra steps to verify your ID before extending credit (available online only).
- Credit Report Lock[3] Allows users to limit access to their Equifax credit report by third parties, with certain exceptions.
- Internet Scanning[4] Monitors suspicious web sites for your Social Security, Passport, Credit Card, Bank, and Insurance Policy Numbers, and alerts you if your private information is found there.
- Lost Wallet Assistance. If you lose your wallet, we'll help you cancel and re-issue your cards and ID
- Up to $1 MM in identity theft insurance[5]
- Live agent Customer Service 7 days a week from 8 a.m. to 3 a.m.
- Identity Restoration If you become a victim of identity theft, an Equifax identity restoration specialist will work on your behalf to help you restore your identity. Call the number within your online member center for assistance.

[1]Credit monitoring from Experian® and Transunion® will take several days to begin.

[2]The Automatic Fraud Alert feature made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.

[3]Locking your Equifax credit file with Credit Report Control will prevent access to your Equifax credit file by certain third parties, such as credit grantors or other companies and agencies. Credit Report Control will not prevent access to your credit file at any other credit reporting agency, and will not prevent access to your Equifax credit file by companies like Equifax Global Consumer Solutions which provide you with access to your credit report or credit score or monitor your credit file; Federal, state and local government agencies; companies reviewing your application for employment; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; for fraud detection and prevention purposes; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com.

[4]Internet scanning will scan for your Social Security number (if you choose to), up to 5 bank accounts, up to 6 credit/debit card numbers that you provide, up to 3 email addresses, up to 10 medical ID numbers, and up to 5 passport numbers. Internet Scanning scans thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and is constantly adding new sites to those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guaranteed that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded.

[5] Identity theft insurance is underwritten by American Bankers Insurance Company of Florida or its affiliates. The description herein 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.

EQUIFAX®

How to Enroll: You can sign up online.

To sign up online for online delivery go to www.myservices.equifax.com/patrol.

1. **Welcome Page:** Enter the Activation Code provided at the top of this page in the "Activation Code" box and click the "Submit" button.
2. **Register:** Complete the form with your contact information (name, gender, home address, date of birth, Social Security Number and telephone number) and click the "Continue" button.
3. **Create Account:** Complete the form with your email address, create a User Name and Password, after reviewing the Terms of Use, check the box to accept and click the "Continue" button.
4. **Verify ID:** The system will then ask you up to four security questions to verify your identity. Please answer the questions and click the "Submit Order" button.
5. **Order Confirmation:** This page shows you your completed enrollment. Please click the "View My Product" button to access the product features.

Directions for placing a Fraud Alert

A fraud alert is a consumer statement added to your credit report. This statement alerts creditors of possible fraudulent activity within your report as well as requests that they contact you prior to establishing any accounts in your name. Once the fraud alert is added to your credit report, all creditors should contact you prior to establishing any account in your name. To place a fraud alert on your credit file, visit: www.fraudalerts.equifax.com or you may contact the Equifax auto fraud line at 1-877-478-7625, and follow the simple prompts. Once the fraud alert has been placed with Equifax, a notification will be sent to the other two credit reporting agencies, Experian and Trans Union, on your behalf.