NOTICE OF DATA BREACH

On May 31, 2023, Boot World notified employees, via email, regarding a cyber security breach of confidential information. This notice provides additional information and options for further protection of your identity.

What Happened?
Boot World was recently exposed to a security breach through Paycom, on Saturday, May 27, 2023, around 3:00 AM. Unauthorized parties hacked into our web-based payroll program, Paycom. The culprits gained access to sensitive and confidential information without Boot World's consent.

What Information Was Involved?
The culprits exported an Excel file including employee names, social security numbers, addresses, email addresses, and phone numbers. The attack was carried out at the administrator level. Therefore, they had visibility on direct deposit banking/routing information, tax forms, earning statements, and employee profiles in Paycom. This breach did not expose personnel files.

What Are We Doing?
Boot World is taking this very seriously. We are allowing employees to use 2.00 hours of paid time, at the manager's discretion, depending on the workload in each department and store volume, to contact their financial institutions and credit bureau reporting agencies. We are working diligently with law enforcement and the FBI to investigate this incident while providing our team with guidance and protection. We will keep you updated on further developments.

What You Can Do.

1. Contact the major credit reporting agencies to place a fraud alert or credit freeze, and both services are free of charge.

   Fraud Alert: A security alert, on your credit report, you can add a telephone number so lenders can call you when they receive an application and verify that it's you who is applying. You also can request additional free credit reports when you add an initial security alert or victim statement. Reviewing your report can help you determine whether you are a victim and help you take appropriate action.

   Credit Freeze: A credit freeze, also known as a security freeze, is a tool designed to help protect you from fraud and identity theft. It limits access to your credit report unless you lift the freeze, or "thaw" your credit. Having a freeze in place won't affect your credit scores, but it will keep your credit report from being accessed to calculate scores unless you first lift the freeze.

You must contact each national credit bureaus individually to freeze (or unfreeze) your credit reports. Each credit bureau will do a credit freeze for free upon request. Each credit bureau allows online and phone credit freeze requests.

Equifax
(888) 836-6351
https://www.equifax.com/personal/credit-report-services/credit-freeze/

Experian
(888) 397-3742
https://www.experian.com/freeze/center.html

TransUnion
(800) 680-7289
https://www.transunion.com/credit-freeze

You're entitled to at least one free credit report from each credit bureau periodically using www.AnnualCreditReport.com. We are informed that through 2023, reports are available weekly. Review your reports for signs of trouble, especially the following:

- New accounts that you didn't open.
- Credit inquires that don't match when you applied for credit.
- Balances that do not match your statements.

2. Notify your financial institutions of the security data breach and obtain recommendations for protecting your bank and credit card accounts.

3. Closely monitor your credit card activity. Freezing your social security number can stop new accounts from being opened in your name, but it will not prevent fraudulent charges on an existing account. Protect yourself in these ways:
    - Stay on top of your credit card statements. Look for charges that you do not recognize. There is often a phone number listed along with the merchant's name for each transaction.
    - Sign up for text or email alerts about credit card transactions.
    - If you see a suspicious charge, call your credit card company immediately to dispute it.

Please contact Human Resources with any questions or concerns.
Nicole Ekstrom, Human Resources & Payroll Manager
P: (858) 324-6338
nekstrom@bootworld.com

Boot World values your privacy and deeply regrets that this incident occurred. Boot World is conducting a thorough review of the potentially affected identity records and will notify you if there are any significant developments. Boot World has implemented additional security measures designed to prevent a recurrence of such an attack, and to protect the privacy of Boot World's valued employees.

_____

Employee Name (print) Signature Date