Date: July 29, 2019

Re: Personal Information Potentially Compromised

We are writing to tell you about a data security incident that may have exposed some of your personal information. While we have no reason to believe that this information has been or will be used inappropriately, we would like to let you know what happened, what information was involved, what we have done to address the situation, and to remind you of what you can do to protect your continued privacy.

What Happened?

On or about May 22, 2019, one of our employees received an email that was carefully crafted to appear to be from one of our recruiting vendors, Workable, with a link. The link led to a website requesting the employee's Outlook login credentials. Unfortunately, this email was fraudulent and did not actually come from within our company or Workable. Rather, it was a "phishing" email from a person or entity outside the company that clearly made the email appear as if it came from Workable, and caused our employee to provide her login credentials. We have confirmed that this outside entity used the login credentials to gain access to our employee's Outlook account.

On or about June 13, 2019, we discovered that the employee's Outlook account included a file containing personal information of other employees. We have no reason to believe this file was accessed by the outside entity or sent outside the company. We are sending this notice, however, out of an abundance of caution. We sincerely apologize for any inconvenience or concern this may cause.

What Information Was Involved?

The personal information in the file mentioned above contained your name and social security number. Again, we have no indication to date that that file was taken or even accessed, and we have not received any reports of improper use of any of this information.

What We Are Doing?

We take this type of situation very seriously and promptly investigated the incident. As an initial action, we immediately had the employee change and reset her Outlook password to prevent any further access. In addition, we blocked any further incoming messages from the domain name of the entity that sent the fraudulent email.

Relatedly, we had already been engaged in efforts to prevent harms from such phishing efforts, including, before this incident, initiating mandatory Phishing Training for all employees that have a company network account. The occurrence of this event underscores the importance of employees to be vigilant for phishing attempts.

We are also taking this opportunity of this notice to remind everyone about the critical importance that each employee plays in this security effort and ask all employees to be very careful in responding to emails that request information to be sent, logon information be given,

or other actions to be taken that can give an outside entity access to company or employee information or systems. If you receive any such email or if an email asks you to do something that seems out of the ordinary, be particularly suspicious and consider contacting the requesting individual by phone or in person to confirm the request, or, if that cannot be done, alert the Help Desk before responding.

What You Can Do?

There are several steps you can take to protect your continued privacy and be sure that the information in the file noted above is not used improperly. Many of these are good practices that you may want to employ in any event.

First, in an abundance of caution, we have arranged with Experian to provide you a two-year subscription for Experian's® IdentityWorksSM.

This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you enroll by: October 31, 2019 (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: **https://www.experianidworks.com/credit]**
- Provide your activation code: **[Unique Code]**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 1-877-890-9332 by October 31, 2019. Be prepared to provide engagement number DB13792 as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is not required for enrollment in Experian IdentityWorks.

You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- Experian credit report at signup: See what information is associated with your credit file. Daily credit reports are available for online members only.*
- Credit Monitoring: Actively monitors Experian file for indicators of fraud.
- Identity Restoration: Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- Experian IdentityWorks ExtendCARETM: You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- Up to $1 Million Identity Theft Insurance**: Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 1-877-890-9332. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for one year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

Second, contact any financial institutions that you bank with and advise them of this situation, particularly if any of them use your social security number to identify or verify you. Regularly check your accounts online or via telephone for any potential fraudulent activity. Always and promptly upon receipt, check your monthly/periodic statements from each of your financial institutions and credit card companies and immediately report to that company any unauthorized or suspicious transactions. Many credit card companies also offer potential fraud alerts that you can received by text or email, and usually for no charge. Sign up for any such program.

For More Information

For general information on protecting your privacy and preventing unauthorized use of your personal information, you may visit the U.S. Federal Trade Commission's Web site, http://ftc.gov or contact your state office of consumer affairs or attorney general. You can also see the attached "Reference Guide" for more information relevant to your state.

* * *

We are committed to maintaining the security and privacy of the personal information you entrusted to us. We apologize for any inconvenience or concern this incident may cause. If we can be of any further assistance or answer any questions, or you encounter any problems that you believe to be related to this incident please call me at the email address below or Jeffrey Annis at (p) 781-585-5165 or (e) jeff.annis@lknife.com.

Sincerely,

Deborah Lahteine
Senior Vice President
781-585-5165
Deb.Lahteine@Sheehancos.com

Reference Guide

In the event that you suspect that you are a victim of identity theft, we encourage you to consider taking the following steps:

Order Your Free Credit Report. To order your free credit report, visit www.annualcreditreport.com, call toll-free at 877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Do not contact the three credit bureaus individually; they provide your free report only through the website or toll-free number.

When you receive your credit report, review the entire report carefully. Look for any inaccuracies and/or accounts you don't recognize, and notify the credit bureaus as soon as possible in the event there are any.

You have rights under the federal Fair Credit Reporting Act ("FCRA"). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov

Place a Fraud Alert on Your Credit File: To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be a victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can report potential identity theft to all three of the major credit bureaus by calling any one of the toll-free fraud numbers below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three bureaus.

Equifax	P.O. Box 740241 Atlanta, Georgia 30374-0241	877-478-7625	www.equifax.com
Experian	P.O. Box 9532 Allen, Texas 75013	888-397-3742	www.experian.com
TransUnion	Fraud Victim Assistance Division P.O. Box 2000 Chester, Pennsylvania 19016	800-680-7289	www.transunion.com

Place a Security Freeze on Your Credit File. You have the right to place a "security freeze" on your credit file. A security freeze generally will prevent creditors from accessing your credit file at the three nationwide credit bureaus without your consent. You can request a security freeze free of charge by contacting the credit bureaus at:

Equifax	P.O. Box 105788 Atlanta, Georgia 30348	www.equifax.com

Experian	P.O. Box 9554 Allen, Texas 75013	www.experian.com
TransUnion	Fraud Victim Assistance Division P.O. Box 2000 Chester, Pennsylvania 19016	www.transunion.com

The credit bureaus may require that you provide proper identification prior to honoring your request. In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.)
2. Social Security number
3. Date of birth
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years.
5. Proof of current address, such as a current utility bill or telephone bill
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to law enforcement agency concerning identity theft

Placing a security freeze on your credit file may delay, interfere with, or prevent timely approval of any requests you make for credit, loans, employment, housing or other services. For more information regarding credit freezes, please contact the credit reporting agencies directly.

Contact the U.S. Federal Trade Commission. If you detect any incident of identity theft or fraud, promptly report the incident to your local law enforcement authorities, your state Attorney General and the Federal Trade Commission ("FTC"). If you believe you identity has been stolen, the FTC recommends that you take these additional steps.

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. Use the FTC's ID Theft Affidavit (available at www.ftc.gov/idtheft) when you dispute new unauthorized accounts.
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.

You can learn more about how to protect yourself from becoming an identity theft victim (including how to place a fraud alert or security freeze) by contacting the FTC:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft

For Iowa Residents: You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. This office can be reached at:

Hoover State Office Building
1305 E. Walnut Street
Des Moines, IA 50319
(515) 281-5164
www.iowaattorneygeneral.gov

For Maryland Residents: You can obtain information from the Maryland Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the Maryland Attorney General at:

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
888-743-0023, www.oag.state.md.us

For Massachusetts Residents: You have a right to request from us a copy of any police report filed in connection with this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. As noted above, you also have the right to place a security freeze on your credit report at no charge.

For North Carolina Residents: You can obtain information from the North Carolina Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the North Carolina Attorney General at:

North Carolina Attorney General's Office
Consumer Protection Division
900 Mail Service Center
Raleigh, NC 27699-9007
(877) 566-7226
www.ncdoj.gov

For Oregon Residents: We encourage you to report suspected identity theft to law enforcement, including the Federal Trade Commission and the Oregon Attorney General. You can contact the Oregon Attorney General at:

Oregon Department of Justice
1162 Court Street NE
Salem, OR 97301-4096
(877) 877-9392
www.doj.state.or.us

For Rhode Island Residents: You can obtain information from the Rhode Island Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the Rhode Island Attorney General at:

Rhode Island Office of the Attorney General
Consumer Protection Unit
150 South Main Street
Providence, RI 02903
(401) 274-4400
www.riag.ri.gov