885 Rt. 67 • Ballston Spa, NY 12020 • 1-800-724-9663
www.curtislumber.com

February 27, 2018

VIA EMAIL AND FIRST CLASS MAIL

Re: *Data Breach on February 5, 2018*

If you are receiving this letter, your information was impacted by the February 5, 2018 Data Breach. This letter has been prepared to provide you with important information as a follow up to our email to you on February 22, 2018.

In response to several employee reports of federal income tax filing issues, we conducted a review of our systems and contacted our business partners who have access to your sensitive personal information to request they do the same.

Early evening on February 23, 2018, we determined that on February 5, 2018, Curtis Lumber Company, Inc. was the subject of a spear phishing incident that resulted in your information being released to an unknown person or persons.

The information released contains your

We believe this information was used to file fraudulent federal income tax returns for a handful of employees, and to establish pre-paid debit accounts with GreenDot. We have already reported this incident to the IRS and the applicable state tax and law enforcement authorities in an effort to prevent any further misuse of your for income tax filing purposes.

If you have been impacted by this, please notify Nicole Huggins in HR at 518-490-1413.

Curtis Lumber Company, Inc. will reimburse for (1) one year of coverage through LifeLock Ultimate Plus. This service will need to be set up by you individually. Please contact Pam Stott [pamelas@curtislumber.com, 518-490-1423] if you have or intend to obtain this service. Once notified, we will reimburse the expense in your next paycheck. Please forward your proof of the annual service payment to Pam Stott.

We also advise you to immediately take the following steps:

1. **Contact the IRS if you have not filed your return yet, or if you have experienced any issues filing your federal income tax return**.

The IRS requires anyone who has issues with their 2017 tax return to fill out an IRS Form 14039. Form 14039 can be submitted along with a paper tax return and accompanying information or alone if you have already filed electronically. According to the IRS, it is critical that you be responsive with their investigation efforts in order to better allow them to expedite the processing of your income tax return after submitting a completed Form 14039

2. **Contact one of the three major credit bureaus**.

We recommend that you call the toll-free numbers of any one of the three major credit bureaus (below) to place a fraud alert on your credit report. This can help prevent an identity thief from opening additional accounts in your name. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. Additional information is available at http:// www.annualcreditreport.com. As soon as one of the credit bureaus confirms your fraud alert, the other two credit bureaus will automatically be notified to place alerts on your credit report, and all three reports will be sent to you free of charge.

Equifax: 1-800-525-6285; www.equifax.com; P.O. Box 740241, Atlanta, GA 30374-0241	**Experian**: 1-888-EXPERIAN (397-3742); www.experian.com; P.O. Box 9532, Allen, TX 75013	**TransUnion**: 1-800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790

3. **Obtain your credit report**.

We also recommend you order your credit report. By establishing a fraud alert, you will receive a follow-up letter that will explain how you can receive a free copy of your credit report. When you receive your credit report, examine it closely and look for signs of fraud, such as credit accounts that are not yours.

4. **Be vigilant and continue to monitor your accounts and credit reports**.

Even if a fraud alert is or has been placed on your account, you should continue to monitor your accounts and credit report to ensure an imposter has not opened an account with your personal information.

5. **Get additional information**.

As indicated in our February 22 email, if you would like additional information, the Federal Trade Commission ("FTC"), IRS and NYS Attorney General each have a webpage dedicated to identity theft.

You may wish to review the tips provided by the FTC on how to avoid identity theft. For more information, please visit http://www.ftc.gov/idtheft or call 1-877-ID-THEFT (877-438-4338).
A copy of "Taking Charge: What to Do if Your Identity is Stolen," a comprehensive guide from the FTC to help you guard against and deal with identity theft, can be found on the FTC's website at: http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.shtm. Further, you can report identity theft to the FTC at: http://www.identitytheft.gov or by calling 1-877-438-4338/1-866-653-4261 (TTY)
The IRS's website can be found here: https://www.irs.gov/identity-theft-fraud-scams/identity-protection.
The NYS Attorney General's website can be found here: https://ag.ny.gov/consumer-frauds-bureau/identity-theft.
You may call 518-885-5311 and ask for the Human Resources department during normal business hours with any questions you have.

We take very seriously our role of safeguarding your personal information and using it in an appropriate manner. We apologize for any inconvenience and concern this situation has caused you and we are doing everything we can to rectify the situation.

Sincerely,

Jay S. Curtis
President