

Joshua P. Brian
T: (850) 205-3336 F: (850) 681-9792
joshua.brian@nelsonmullins.com

215 South Monroe Street, Suite 400
Tallahassee, FL 32301
T: 850.681.6810 F: 850.681.9792
nelsonmullins.com

September 27, 2019

Via Registered Mail and E-mail (attorneygeneral@doj.nh.gov)

Attorney General Gordon J. MacDonald
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

RE: Data Security Incident Notification

Dear Attorney General Gordon J. MacDonald:

I am writing to inform you of a data security incident that may affect nine (9) New Hampshire residents, as detailed below. Our client, John Lucas Tree Expert Co., P.O. Box 958, Portland, ME 04104, a tree and vegetation management service, will be sending the attached written notices with an offer to enroll in a 12-month Equifax identity monitoring product at no cost.

On July 16, 2019, Lucas Tree was informed an unauthorized individual used a spoofed e-mail address designed to appear like its company e-mail addresses in an attempt to trick unsuspecting persons into paying the unauthorized individual.

As a result of this incident, Lucas Tree engaged an industry-leading forensic investigation firm to investigate whether there was any compromise to its information technology environment. The investigation revealed that an unauthorized user created a contact in a company O365 e-mail account on August 27, 2018, and created an unauthorized mail forwarding rule in the subject account on August 29, 2018, which was discovered and deleted on July 17, 2019. There was no evidence that the unauthorized individual accessed the account between April 25, 2019, and July 24, 2019. Based upon available forensic evidence, the forensic investigation firm was unable to determine what e-mails were accessed or acquired by the unauthorized individual.

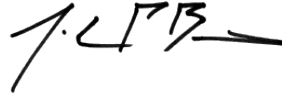
Due to the forensic investigation firm's findings, Lucas Tree retained an additional firm to review all available data within the e-mail account, which, after addition of contact information, was completed on September 13, 2019, and revealed some e-mails and attachments contained personal information. With respect to the New Hampshire residents, the personal information was either a Social Security number or Driver's License number. While Lucas Tree has no knowledge that any personal information was accessed or acquired by an unauthorized individual, and no knowledge of any resulting identity theft, fraud, or financial losses to any individual, it has decided to proactively provide notice and one year of identity monitoring without cost to the New

September 27, 2019
Page 2

Hampshire residents whose personal information was located within the e-mail account. A copy of the September 27, 2019, notice is enclosed with this letter.

Please let me know if you have any additional questions regarding the notification.

Very truly yours,

A handwritten signature in black ink, appearing to read 'J.P. Brian', with a horizontal line extending to the right.

Joshua P. Brian

Enclosure: Notice Letter



Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

NOTICE OF DATA BREACH

Dear <<Name 1>>:

John Lucas Tree Expert Co. (“Lucas Tree Experts”) respects the privacy of your information, which is why we are writing to tell you about a data security incident that may have exposed some personal information of a small number of individuals, including yours. We take the protection and proper use of your information very seriously. For this reason, we are contacting you directly to explain the circumstances of the data security incident.

What Happened

On July 16, 2019, we were informed an unauthorized individual used a spoofed e-mail address designed to appear like our company e-mail addresses in an attempt to trick unsuspecting persons into paying the unauthorized individual.

As a result of this incident, we engaged an industry-leading forensic investigation firm to investigate whether there was any compromise to our information technology environment. The investigation revealed that an unauthorized user created a contact in a company e-mail account on August 27, 2018, and created an unauthorized mail forwarding rule in the subject account on August 29, 2018, which was discovered and deleted on July 17, 2019. There was no evidence that the unauthorized individual accessed the account between April 25, 2019, and July 24, 2019. Based upon available forensic evidence, the forensic investigation firm was unable to determine what e-mails were accessed or acquired by the unauthorized individual.

Due to the forensic investigation firm’s findings, we retained an additional firm to review all available data within the e-mail account, which, after addition of contact information, was completed on September 13, 2019, and revealed some e-mails and attachments contained personal information. While we have no knowledge that any of your personal information was accessed or acquired by an unauthorized individual, we have decided to proactively provide notice and one year of identity monitoring without cost to you to ensure you can protect yourself.

What Information Was Involved

As a result of this security incident, some of your personal information may have been accessed and acquired without authorization, which may have included your first and last name, address, <<ClientDef1(Breach Details Variable Text)>>.

We are notifying you so you can take appropriate steps to protect your personal information.

What We Are Doing

To help relieve concerns following this incident, we have secured Equifax to provide identity monitoring at no cost to you for one year. Equifax, as a credit bureau with over a billion updates to data sets daily, functions as a first point of contact for credit related issues, which allows it to efficiently furnish timely notification to individuals enrolled in its identity monitoring product.

Visit www.myservices.equifax.com/gold to activate and take advantage of your identity monitoring product.

You have until <<EnrollmentDate>> to activate your identity monitoring product.

Equifax Credit Watch Gold Activation Code Number: <<ACTIVATION CODE>>

Additional information describing this product is included with this letter. We encourage you to review the description and to consider enrolling in this product.

To further protect your information from unauthorized access, we have implemented heightened technical security measures designed to prevent similar incidents from occurring in the future.

What You Can Do

Please review the enclosed “**Additional Resources**” section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

For More Information

For further information, please call 855-913-0608 between 9:00 a.m. and 9:00 p.m. EST. We take the protection of your personal information very seriously and apologize for any inconvenience. We trust that the services we are offering to you demonstrate our continued commitment to your security and satisfaction.

Sincerely,

Human Resources Department
Lucas Tree

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies is:

Equifax, P.O. Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, P.O. Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, P.O. Box 34012, Fullerton, CA 92834, www.transunion.com, 1-800-916-8800

Free Credit Report. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for unauthorized activity over the next twelve to twenty-four months, and immediately report incidents of suspected identity theft to both your financial provider and law enforcement.

You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies. You may also seek to have information relating to fraudulent transactions removed from your credit report. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alert. You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies above. A fraud alert tells creditors to follow certain procedures, including contacting you before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit.

Security Freeze. You have the ability to place a security freeze on your credit report free of charge.

A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line, or a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; (5) legible copy of a government issued identification card; (6) legible copy of a recent utility bill or bank or insurance statement that displays your name and current mailing address, and the date of issue; and (7) any applicable incident report or complaint with a law enforcement agency.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

State Attorney General's Office Contact Information:

<<ClientDef2(State AG Office Info)>>.