McDonald Hopkins
A business advisory and advocacy law firm®

Dominic A. Paluzzi
Direct Dial: 248.220.1356
dpaluzzi@mcdonaldhopkins.com

McDonald Hopkins PLC
39533 Woodward Avenue
Suite 318
Bloomfield Hills, MI 48304
P 1.248.646.5070
F 1.248.646.5075

December 10, 2018

VIA U.S. MAIL

Attorney General Gordon MacDonald
Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

Re: Beecher Carlson – Incident Notification

Dear Attorney General MacDonald:

McDonald Hopkins PLC represents Beecher Carlson, a subsidiary of Brown & Brown, Inc. I write to provide notification regarding an incident that may involve the personal information of approximately five (5) New Hampshire residents. Beecher Carlson's investigation is ongoing and this notification will be supplemented with any new significant facts or findings subsequent to this submission, if any. By providing this notice, Beecher Carlson does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

Beecher Carlson recently learned that emails within an employee's email account may have been forwarded to an external email address not affiliated with Beecher Carlson. Beecher Carlson immediately launched an investigation to analyze the extent of any compromise to the email account and the security of the emails and attachments contained within. After an extensive investigation, Beecher Carlson's information technology team concluded that it was possible that an unauthorized individual may have had access to the emails contained in the impacted email account.

Beecher Carlson devoted considerable time and effort to determine what information was contained in the affected email account. Based on its comprehensive investigation and document review, which concluded on November 27, 2018, Beecher Carlson discovered that the compromised email account contained the affected residents' full names and drivers' license numbers. The affected residents' Social Security numbers were not impacted by this incident.

To date, Beecher Carlson has no evidence that any of the information has been misused. Nevertheless, out of an abundance of caution, Beecher Carlson wanted to make you (and the affected residents) aware of the incident and explain the steps it is taking to safeguard the affected residents from identity theft. Beecher Carlson will provide the affected residents with notice of this incident on December 11, 2018 in substantially the same form as the letter attached

hereto. Beecher Carlson is offering the affected residents a complimentary one-year membership with a credit monitoring service. Beecher Carlson is advising the affected residents to remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. Beecher Carlson is providing dedicated call center support to answer the affected residents' questions. Beecher Carlson is advising the affected residents about the process for placing a fraud alert and/or security freeze on their credit files, and obtaining a free credit report. The affected residents are also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

Beecher Carlson is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. Beecher Carlson continually evaluates and modifies its practices and internal controls to enhance the security and privacy of personal information.

Should you have any questions regarding this notification, please contact me at (248) 220-1356 or *dpaluzzi@mcdonaldhopkins.com*.

Sincerely,

Dominic A. Paluzzi

Encl.

BEECHER CARLSON

Notice of Data Breach

[redacted]

[redacted]

Dear [redacted]

I am writing to provide you with important details about a recent incident at Beecher Carlson, a subsidiary of Brown & Brown, Inc, involving the security of your information and the measures we are taking to protect your information.

What Happened?

We recently learned that emails within one of our employee's email accounts may have been forwarded to an external email address not affiliated with us.

What We Are Doing.

We immediately launched an investigation to analyze the extent of any compromise to the email accounts and the security of the emails and attachments contained within. After an extensive investigation, our information technology team concluded that it was possible that an unauthorized individual may have had access to the emails contained in the impacted email account.

What Information Was Involved?

We devoted considerable time and effort to determine what information was contained in the affected email accounts. Based on our comprehensive investigation and document review, which concluded on November 27, 2018, we discovered that the compromised email accounts contained your full name and drivers' license number. Your Social Security number was not impacted by this incident.

What You Can Do.

Although these certain emails were forwarded to an unauthorized email account, we have no evidence that any of the information has been misused. However, out of an abundance of caution, we wanted to make you aware of the incident and suggest steps that you should take to protect yourself. Further, you should remain vigilant in reviewing your financial account statements for fraudulent or irregular activity on a regular basis.

To protect you and your information, we are providing you with 12 months of free credit monitoring and identity theft protection services through TransUnion. This service helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. This service is completely free to you and enrolling in this program will not hurt your credit score. For more information on identity theft prevention, including instructions on how to activate your complimentary one-year membership, please see the additional information provided in this letter.

We take the security of personal information very seriously and apologize for any inconvenience this incident may cause you. We are committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your personal information.

For More Information.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at [redacted]. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against misuse of your information. The response line is available Monday through Friday, 9 a.m. to 9 p.m. Eastern Time.

Sincerely,

[redacted]

Beecher Carlson

– ADDITIONAL PRIVACY SAFEGUARDS INFORMATION –

1. Enrolling in Complimentary 12-Month Credit Monitoring.

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*my*TrueIdentity) for one year provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies.

To enroll in this service, go to the *my*TrueIdentity website at [redacted] and in the space referenced as "Enter Activation Code" enter the following 12-letter Activation Code [redacted] and follow the three steps to receive your credit monitoring service online within minutes.

You can sign up for the online credit monitoring service anytime between now and [redacted]. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion, or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

Once you are enrolled, you will be able to obtain one year of unlimited access to your TransUnion credit report and credit score. The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more. The service also includes access to an identity restoration program that provides assistance in the event your identity is compromised to help you restore your identity and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

If you believe you may be a victim of identity theft, please call the TransUnion Fraud Response Services toll-free hotline at [redacted]. When prompted, enter the following 6-digit telephone pass code [redacted] to speak to a TransUnion representative about your identity theft issue.

2. Placing a Fraud Alert

Whether or not you choose to use the 12 month credit monitoring services offered above, we recommend that you place an initial 90-day "Fraud Alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others. Alternatively, you may file the Fraud Alert online. Here is a link to the Experian fraud alert home page: https://www.experian.com/fraud/center.html.

Equifax
P.O. Box 105069
Atlanta, GA 30348
www.equifax.com
1-800-525-6285

Experian
P.O. Box 2002
Allen, TX 75013
www.experian.com
1-888-397-3742

TransUnion LLC
P.O. Box 2000
Chester, PA 19016
www.transunion.com
1-800-680-7289

3. Consider Placing a Security Freeze on Your Credit File

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "Security Freeze" be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by sending a request in writing or by mail, to all three nationwide credit reporting companies. To find out more about how to place a security freeze, you can use the following contact information:

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion Security Freeze**
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
https://www.freeze.equifax.com	http://experian.com/freeze	http://www.transunion.com/securityfreeze
1-800-685-1111	1-888-397-3742	1-888-909-8872

In order to place the security freeze, you'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit monitoring company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

4. Obtaining a Free Credit Report

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify that all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

5. Additional Helpful Resources

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

Iowa Residents: You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity Theft: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, Telephone: (515) 281-5164

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Department of Justice, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 877-566-7226.

Oregon Residents: You may obtain information about preventing identity theft from the Oregon Attorney General's Office: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392