



Alyssa R. Watzman
1700 Lincoln Street, Suite 4000
Denver, Colorado 80203
Alyssa.Watzman@lewisbrisbois.com
Direct: 720.292.2052

January 16, 2020

VIA E-MAIL

Gordon MacDonald, Attorney General
Consumer Protection and Antitrust Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03301
Email: DOJ-CPB@doj.nh.gov

Re: Notice of Data Security Incident

Dear Attorney General MacDonald:

We represent Hallier Benefit Advisors (“HBA”), an insurance agency located in North Kansas City, Missouri that specializes in the marketing and maintenance of employee and executive benefit programs. This letter is being sent because personal information belonging to certain New Hampshire residents may have been affected by a recent data security incident experienced by HBA. The affected information may have included New Hampshire residents’ names and Social Security numbers.

On September 26, 2019, HBA discovered unusual activity in one HBA employee email account. HBA immediately took steps to secure the account and launched an investigation with the assistance of a digital forensics firm to determine what happened and whether personal information had been accessed or acquired without authorization as a result. On October 1, 2019, the forensics firm reported that one HBA employee email account had been accessed without authorization. HBA then launched a data review project to determine whether that account contained personal information. On November 21, 2019, the data review project revealed that the personal information of New Hampshire residents was contained within the account. HBA then worked diligently to identify up-to-date address information required to notify potentially impacted individuals.

HBA notified four (4) potentially affected New Hampshire residents via the attached sample letter on January 15, 2020. In so doing, HBA offered notified individuals twelve (12) months of complimentary credit monitoring and identity theft restoration services through Kroll, a global leader in risk mitigation and response.

January 16, 2020
Page 2

Please contact me should you have any questions.

Sincerely,

/s/ Alyssa R. Watzman

Alyssa R. Watzman of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Enclosure: Consumer Notification Letter



<<Date>> (Format: Month Day, Year)

<<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

Re: Notification of Data Security Incident

Dear <<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>,

We are writing to inform you of a data security incident experienced by Hallier Benefit Advisors (“HBA”)¹ that may have affected your personal information. As explained below, we recently learned that an unauthorized individual gained access to an HBA employee email account containing your personal information. We are writing to notify you of this incident, to offer you complementary credit monitoring and identity theft restoration services, and to inform you about steps that can be taken to help protect your personal information.

What Happened? On September 26, 2019, we detected unusual activity in an HBA employee email account caused by an unknown third-party with unauthorized access to the account. We immediately took steps to secure the account and launched an investigation. In connection therewith, we engaged a leading, independent forensics firm to determine what happened and whether sensitive information was accessed or acquired without authorization. On November 21, 2019, our investigation determined that the impacted HBA email account contained some of your personal information which may have been viewed or accessed by the unauthorized individual.

Please note that this unauthorized access was limited to information transmitted via email and did not affect any other information systems. Moreover, we are not aware of the misuse of any of your personal information.

What Information Was Involved? The following information may have been contained within the accessed email account: your <<ClientDef1(Impacted Data)>>.

What Are We Doing? As soon as we discovered this incident, we took the measures referenced above. We also implemented enhanced security measures applicable to our email system in order to better safeguard all personal information in our possession and to help prevent a similar incident from occurring in the future. In addition, we reported this matter to the Federal Bureau of Investigation and will provide whatever assistance is necessary to hold the perpetrators of this incident accountable. Finally, we are offering you complementary credit monitoring and identity theft restoration services through Kroll, a global leader in risk mitigation and response. These services include Credit Monitoring, \$1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

What Can You Do? We recommend that you activate your complementary Kroll services. Activation instructions and a description of the services being provided are included with this letter. We also recommend that you review the guidance included with this letter about how to protect your personal information.

For More Information. If you have questions or need assistance, please contact Kroll at 1-???-???-????, Monday through Friday from 8 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays. Kroll representatives are fully versed on this incident and can answer any questions you may have regarding the protection of your personal information.

¹HBA was formerly affiliated with Hallier Reed, which provided services to your current or former employer and thus may have been in possession of your personal information as a result of those services provided thereto.

Please accept our sincere apologies and know that we deeply regret any worry or inconvenience that this may cause you.

Sincerely,

A handwritten signature in black ink, appearing to read "S. Hallier". The signature is fluid and cursive, with a long horizontal stroke extending to the right.

Scott Hallier, Agency Principal
Hallier Benefit Advisors

Steps You Can Take to Further Protect Your Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print this form at <https://www.annualcreditreport.com/cra/requestformfinal.pdf>. You also can contact one of the following three national credit reporting agencies:

TransUnion P.O. Box 1000 Chester, PA 19016 1-877-322-8228 www.transunion.com	Experian P.O. Box 9532 Allen, TX 75013 1-888-397-3742 www.experian.com	Equifax P.O. Box 105851 Atlanta, GA 30348 1-800-525-6285 www.equifax.com	Free Annual Report P.O. Box 105281 Atlanta, GA 30348 1-877-322-8228 annualcreditreport.com
---	---	--	---

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for one (1) year. 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. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: You have the right to put a security freeze on your credit file. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. There is no charge to place, lift or remove the security freeze. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC or from your respective state Attorney General about steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state. Residents of Maryland, North Carolina, and Rhode Island can obtain more information from their Attorneys General using the contact information below.

Federal Trade Commission 600 Pennsylvania Ave, NW Washington, DC 20580 consumer.ftc.gov , and www.ftc.gov/idtheft 1-877-438-4338	Maryland Attorney General 200 St. Paul Place Baltimore, MD 21202 oag.state.md.us 1-888-743-0023	North Carolina Attorney General 9001 Mail Service Center Raleigh, NC 27699 ncdoj.gov 1-877-566-7226	Rhode Island Attorney General 150 South Main Street Providence, RI 02903 http://www.riag.ri.gov 401-274-4400
---	---	---	--

You also have certain rights under the Fair Credit Reporting Act (FCRA), including: to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information, as well as others. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

As referenced above, we have secured the services of Kroll to provide credit monitoring and identity theft restoration services at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your services² include Credit Monitoring, \$1 Million Identity Fraud Loss Reimbursement Fraud Consultation, and Identity Theft Restoration.

How to Activate Your Services

Visit <<ID Monitoring URL>> to activate and take advantage of your credit monitoring and identity theft restoration services.

You have until <<Date>> to activate your credit monitoring and identity theft restoration services.

Membership Number: <<Member ID>>

If you have questions, please call 1-???-???-????, Monday through Friday from 8 a.m. to 5:30 p.m. Central Time.

Take Advantage of Your Services

You've been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

\$1 Million Identity Fraud Loss Reimbursement

Reimburses you for covered, out-of-pocket expenses totaling up to \$1 million for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

² Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.