BakerHostetler

Baker&Hostetler LLP

312 Walnut Street
Suite 3200
Cincinnati, OH 45202-4074

T 513.929.3400
F 513.929.0303
www.bakerlaw.com

Patrick H. Haggerty
direct dial: 513.929.3412
phaggerty@bakerlaw.com

August 3, 2018

Via Email (SecurityBreach@atg.wa.gov)
And First Class Mail

Attorney General Bob Ferguson
Office of the Washington Attorney General
Consumer Protection Division
800 5th Ave, Suite 2000
Seattle, WA 98104-3188

Re: Incident Notification

Dear Sir or Madam:

We are writing on behalf of our client, Colorado Bankers Life Insurance Company ("CBLife"), to notify you of a security incident involving Washington residents.

On June 14, 2018, CBLife completed the forensic aspect of its investigation of a data security incident that involved a targeted phishing attack that compromised 6 cloud-based employee email accounts at various times between the dates of March 28, 2018 and April 13, 2018. Upon discovery, CBLife secured the potentially affected employee email accounts, changed account settings to enhance security, and engaged a leading cyber security firm to assist with the investigation. For one of these accounts, the investigation was able to determine the emails and attachments that had been accessed by the unauthorized individual(s). For the remaining accounts, the investigation was unable to determine the scope of information that may have been accessed or acquired by the individual(s). The investigation confirmed that CBLife's internal network and systems were not affected.

CBLife then undertook a comprehensive review of the emails in the employees' email accounts and determined that an email or attachment contained certain information about some of its employees, producers, advisors, and policyholders. This information varies among individuals, but includes names along with one or more of the following: Social Security number, payment card number, and financial account numbers. On June 20, 2018, CBLife learned that there were Washington residents' personal information in the email accounts. To date, CBLife is not aware of any misuse of the information.

Beginning on August 3, 2018, CBLife will mail notification letters to 956 Washington residents, in accordance with Wash. Rev. Code § 19.255.010, via United States Postal Service First-Class mail, in substantially the same form as the enclosed letter. CBLife will be offering eligible individuals a complimentary, one-year membership to a credit monitoring and identity theft protection service through TransUnion®. CBLife has also notified law enforcement and will continue to support any investigation.

To help prevent a similar incident from occurring in the future, CBLife is providing additional extensive training to its employees regarding phishing emails and other cybersecurity issues. In addition, CBLife has enhanced existing security measures by implementing multi-factor authentication for email.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

Patrick H. Haggerty
Partner

Enclosure

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

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

<<Date>>

Dear <<Name 1>>:

Colorado Bankers Life Insurance Company ("CBLife") understands the importance of protecting the personal information of its employees, producers, advisors, and policyholders. We are writing to inform you that we recently identified and addressed a security incident that may have involved your personal information. This notice explains the incident, measures we have taken, and some steps you can take in response.

What Happened: On June 20, 2018, CBLife completed its investigation of a data security incident that involved a targeted phishing attack that compromised some of its employees' cloud-based email accounts at various times between the dates of March 28, 2018 and April 13, 2018. Upon discovery, we secured employee email accounts, changed account settings to enhance security, and engaged a leading cyber security firm to assist with the investigation. CBLife undertook a comprehensive review of the emails and attachments in the accounts. The investigation confirmed that CBLife's internal network and systems were not affected.

<<Data Element Paragraph>>

What You Can Do: To date, CBLife is not aware of any misuse of the information or any other criminal activity as a result of the phishing attack. However, we encourage you to remain vigilant by reviewing your account statements for any unauthorized activity. As a precaution, CBLife has arranged for you to enroll in a complimentary, 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. **For more information on *my*TrueIdentity, including instructions on how to activate your complimentary one-year membership, as well as some additional steps you can take to protect your information, please see the page that follows this letter.**

What We are Doing: We apologize for any concern or inconvenience this incident may cause. To help prevent a similar incident from occurring in the future, we have provided extensive training to our employees regarding phishing emails and other cybersecurity issues. In addition, we enhanced existing security measures by implementing multi-factor authentication for email.

For More Information: If you have questions about this matter, please call 866-778-1149, Monday through Friday between 9:00 am and 9:00 pm Eastern Time.

Sincerely,

Jeffrey L. Levin
President, Colorado Bankers Life Insurance Company

*MY*TRUEIDENTITY ENROLLMENT INSTRUCTIONS

To enroll in this service, go to the *my*TrueIdentity website at **www.mytrueidentity.com** and in the space referenced as "Enter Activation Code", enter the following 12-letter Activation Code <<Insert Unique 12- letter Activation Code>> and follow the three steps to receive your credit monitoring service online within minutes.

If you do not have access to the Internet and wish to enroll in a similar offline, paper based, credit monitoring service, via U.S. Mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at 1-855-288-5422. When prompted, enter the following 6-digit telephone pass code <<Insert static 6-digitTelephone Pass Code>> and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and <<Insert Date>>. 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 that 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.)

MORE WAYS TO PROTECT YOURSELF

Even if you choose not to take advantage of this free credit monitoring, we recommend that you remain vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
Experian, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

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 state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

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

If you are a resident of Maryland or North Carolina, you may contact and obtain information from your state attorney general at:

Maryland Attorney General's Office, 200 St. Paul Place, Baltimore, MD 21202
www.oag.state.md.us, 1-888-743-0023 (toll free when calling within Maryland)
1-410-576-6300 (for calls originating outside Maryland)

North Carolina Attorney General's Office, 9001 Mail Service Center, Raleigh, NC 27699, www.ncdoj.gov, 1-919-716-6400 or toll free at 1-877-566-7226

If you are a resident of West Virginia, you have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described above. You also have a right to place a security freeze on your credit report, as described above.

Fraud Alerts: There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Credit Freezes: You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally $5 to $20 per action at each credit reporting company. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information.

To place a security freeze on your credit report, you must send a written request to each of the three major reporting agencies by regular, certified, or overnight mail at the addresses below:

Equifax Security Freeze, PO Box 105788, Atlanta, GA 30348, www.equifax.com
Experian Security Freeze, PO Box 9554, Allen, TX 75013, www.experian.com
TransUnion Security Freeze, PO Box 2000, Chester, PA 19016, www.transunion.com

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 the police report, investigative report, or complaint to a law enforcement agency concerning identity theft

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number ("PIN") or password or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.