Blue Cross of Idaho

An Independent Licensee of the Blue Cross and Blue Shield Association

From: DeLange, Brett <brett.delange@ag.idaho.gov>
Sent: Friday, March 19, 2021 3:07 PM
To: Chris Jenkins <Chris.Jenkins@bcidaho.com>
Subject: [EXTERNAL] RE: Follow-Up / Report Per 28-51-105

Thank you.

Brett DeLange
Office of Attorney General
208-334-4114
brett.delange@ag.idaho.gov

From: Chris Jenkins [mailto:Chris.Jenkins@bcidaho.com]
Sent: Friday, March 19, 2021 2:48 PM
To: DeLange, Brett <brett.delange@ag.idaho.gov>
Cc: Brian Wonderlich <Brian.Wonderlich@bcidaho.com>
Subject: Follow-Up / Report Per 28-51-105

Good Afternoon, Brett –

Thank you again for speaking with us earlier regarding the issue we wanted to report under Idaho Code 28-51-105. I am also reaching out to the broker involved separately and asking them to contact you directly and to provide a copy of the member notification that they will be sending as soon as they've finalized the template document. That said, here's a very high level recap based on my understanding of the situation:

One of our brokers, AHT Insurance (Armrfield, Harrison & Thomas) experienced a breach of their cyber security on December 4, 2020 due to a phisphing attack. They discovered the attack on December 8th and shut the account down and started their investigation. They determined on February 5, 2021 that they could not be certain what portions of their database may have been compromised and began notifying all their partners/carriers. BCI received notice of a potential HIPAA breach on February 9th. During the period this was all happening, AHT was acquired by Baldwin Risk Partners, who is handling the investigation along with external counsel Ted Augustino of the law firm Locke Lord.

As Brian shared during the call, BCI was aware of the fact that PHI was involved due to the notice they provided in February. However, we did not know that there was driver's license numbers, SSN's, or potentially other financial

information at risk until this morning. We are providing this notice to you to satisfy the statutory reporting requirements.

At this time there does not appear to be any indication that any data has actually been compromised. Nevertheless, AHT is providing all affected members with a personalized notification letter and credit monitoring as per HIPAA requirements. Since AHT is handling this process, I cannot speak to timing but can share that I saw a draft template of the notification letter, so I would assume the notifications will occur in the near future.

Please do not hesitate to contact me or Brian if you have any questions.

Thank you,

Chris Jenkins
Senior Associate General Counsel
Ph. (986) 224-3385
Cell (541) 321-5703

NOTICE: This email message is for the sole use of the intended recipient(s) and may contain confidential and privileged information. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient, please contact the sender by reply email and destroy all copies of the original message.
Blue Cross of Idaho, 3000 E. Pine Ave, Meridian, ID 83642

AHT INSURANCE
Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

April 12, 2021

G3682-L02-0000002 T00001 P001 *****AUTO**MIXED AADC 159
SAMPLE A. SAMPLE - L02
APT ABC
123 ANY ST
ANYTOWN, ST 12345-6789

Re: Important Notice Regarding Potential Disclosure of Your Personal Information

Dear Sample A. Sample:

Armfield, Harrison & Thomas ("AHT") is contacting you about a security incident involving potential disclosure of your personal information. One of our AHT insurance brokers may have had your personal information for purposes of placing group health insurance and ancillary benefits coverage on behalf of your current or past employer. Certain of your personal information, which was in an email account of our insurance broker may have been subject to compromise in a phishing attack. As a result, and out of an abundance of caution, AHT is notifying you of this incident and providing you with tools to help you protect yourself against potential identify theft.

What Happened
On December 8, 2020, AHT discovered that an apparent phishing attack on December 4, 2021 compromised the credentials of one of our insurance brokers, providing unauthorized access to the insurance broker's email account. AHT immediately terminated the attack and began to investigate. The attack compromised one insurance broker's credentials and permitted an unauthorized person to remotely access the broker's email account. AHT has also confirmed that the unauthorized access was limited to this one insurance broker's email account; there is no compromise of the security of any of AHT's other systems or databases.

After the close of business on Friday, February 5, 2021, AHT learned that the compromised email account included personal information of individuals that had been collected in connection with insurance transactions. Due to the nature and structure of the information contained in the compromised account, we engaged an outside firm to analyze the data to determine the identity of the affected individuals, and the types of information involved in the incident. We also worked to associate the information with relevant insurance carriers, where possible.

What Information Was Involved
Your personal information that was potentially exposed to unauthorized access or acquisition may have included your name, address, date of birth, medical information, health insurance information, other government identification number, and financial account number. We have no indication that your social security number was exposed. We have no indication that your personal information has been misused, but we wanted to make you aware of the incident, our efforts to safeguard your personal information, and resources you may use to protect yourself.

What We Are Doing
We took immediate steps upon the discovery of the attack to terminate the attack and prevent any further unauthorized access to personal information. We have attached instructions to this letter for credit monitoring services we are offering at no cost to you for two years, and information on further steps you can take to protect yourself against identity theft and fraud. We have also been in contact with legal counsel, regulatory authorities, and AHT's insurance carrier partners.

What You Can Do
As always, we recommend that you remain vigilant and review your account statements and credit reports regularly, and report any concerning transactions to your financial services provider. To assist you in protecting yourself against risks related to this incident, we are offering a complimentary two-year membership of Experian's® IdentityWorks℠. Enclosed with this letter is information regarding these services and instructions for enrollment, as well as additional information regarding steps you can take to protect yourself against identity theft and fraud. If you have any questions regarding this incident, please contact our dedicated call center at (866) 506-7888 from Monday through Friday, 6am to 8pm pacific time and Saturdays/Sundays from 8am to 5pm pacific time. To enroll in the credit services we are offering at no cost to you, please contact Experian by following the instructions attached to this letter.

We sincerely apologize for any inconvenience or concern this situation may cause. Again, we want to reassure you that we have taken steps to improve the security of personal information entrusted to us.

Sincerely,

Kate Armfield

Katherine L. Armfield, CPCU
Managing Partner

How to Access Your Credit Monitoring Services

What we are doing to protect your information:
To help protect your identity, we are offering a complimentary two-year membership of Experian's® IdentityWorks℠. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by**: **July 31, 2021** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/credit
- Provide your **activation code**: **ABCDEFGHI**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at (866) 506-7888 by **July 31, 2021.** Be prepared to provide engagement number **DB26572** as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks.
You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Internet Surveillance:** Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at (866) 506-7888. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).
Please note that this Identity Restoration support is available to you for one year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

Additional Information and U.S. State Notification Requirements

There are a number of steps you should consider to guard against identity theft.

Review Your Account Statements and Credit Report: It is recommended that you remain vigilant for incidents of fraud and identity theft by regularly reviewing your account statements and monitoring your credit reports. Report any fraudulent transactions to the creditor or credit reporting agency from whom you received the statement or report. You may obtain a free copy of your credit report from each credit reporting agency once every 12 months, whether or not you suspect any unauthorized activity on your account, by visiting https://www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form available at that website and mailing it to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You may also purchase a copy of your credit report at any time by contacting any one or more of the national credit reporting agencies listed below.

Equifax
P.O. Box 740241
Atlanta, Georgia 30374
www.equifax.com
1-800-685-1111 Credit Reports
1-888-766-0008 Fraud Alert
1-800-685-1111 Security Freeze

Experian
P.O. Box 2002
Allen, TX 75013
www.experian.com
1-888-397-3742 Credit Reports
1-888-397-3742 Fraud Alert
1-888-397-3742 Security Freeze

TransUnion (FVAD)
P.O. Box 105281
Atlanta, GA 30348-5281
www.transunion.com
1-800-888-4213 Credit Reports
1-800-680-7289 Fraud Alert
1-800-680-7289 Security Freeze

Federal Trade Commission (FTC) and State Resources: General guidance on protecting yourself from identify theft is available from the Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Ave. NW, Washington D.C. 20580, by phone at 877-ID-THEFT (438-4338), and/or from the FTC website at http://www.ftc.gov/bcp/edu/microsites/idtheft. In many states, additional information is also available from your state's Attorney General's Office.

Fraud Alerts and Security Freezes: You may obtain information about fraud alerts and security freezes (also referred to as credit freezes), including how to place a fraud alert or security freeze, from the Federal Trade Commission or credit reporting agencies at the contact information provided above. However, be aware that a fraud alert or security freeze may require fees to be paid, may interfere with or delay legitimate requests for credit approval. You'll need to supply your name, address, date of birth, Social Security number and other personal information in order to place a security freeze on your credit.

For residents of Massachusetts:
State law advises you that you have the right to obtain a police report. You also will not be charged for seeking a security freeze, as described above in this document.

For residents of Rhode Island:
To contact the Rhode Island Attorney General; (401) 274-4400 or check http://www.riag.ri.gov/home/ContactUs.php

For residents of Iowa:
State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Oregon:
State law advises you to report any suspected identity theft to law enforcement, as well as the FTC.

For residents of Maryland and North Carolina:
You can obtain information from the Maryland and North Carolina Offices of the Attorney General about steps you can take to avoid identity theft.

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023
www.oag.state.md.us

North Carolina Office of the Attorney General
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
1-877-566-7226
www.ncdoj.com