

January 25, 2019

VIA OVERNIGHT MAIL

Attorney General Gordon J. MacDonald
Office of the Attorney General
State of New Hampshire
33 Capitol Street
Concord, New Hampshire 03301

RECEIVED
JAN 28 2019
CONSUMER PROTECTION

RE: Data Incident Notification

Dear Attorney General MacDonald:

Our firm represents Wausau MedMal Management Services, LLC (“WMMS”), a Wisconsin company that is Plan Manager for the Wisconsin Health Care Liability Insurance Plan (“WHCLIP,” or the “Plan”). WHCLIP hereby formally submits notification of a recent data breach incident, pursuant to N.H. Rev. Stat. Ann. §359-C:20. WHCLIP and WMMS reserve the right to supplement this notice with any new significant details learned subsequent to this submission. By providing this notice, WHCLIP and WMMS do not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire notification of security breach statute, all other laws or personal jurisdiction.

On December 5, 2018, WHCLIP’s accountants advised WHCLIP that an unauthorized third party gained access to a secure file sharing system (Citrix Sharefile) used by accountants for WHCLIP to share financial information required to perform accounting operations as well as statutorily required audits of the Plan. The unauthorized access occurred on November 4, 2018. The unauthorized third party gained access using the login credentials of the independent auditor retained to do the yearly required audit of the Plan’s financial and attendant operations. Logs from Citrix Sharefile indicated that the unauthorized third party downloaded a file containing names, addresses, and Social Security numbers. While there was unauthorized access to Citrix Sharefile, there was no compromise or breach of WHCLIP’s systems or networks, or the systems or networks of WMMS.

Upon learning of the incident, WHCLIP worked with its accountants to investigate the matter. WHCLIP’s accountant immediately terminated the auditor’s access to the secure file sharing system. Additionally, WHCLIP no longer has a relationship with the auditor. In an effort to notify potentially affected individuals quickly, WHCLIP sent an initial letter to those individuals on December 20, 2018, informing them of the unauthorized acquisition of their information. WHCLIP intends to mail potentially affected individuals on January 25, 2019, with further details of the incident and an offer for twelve (12) months of free credit monitoring.

January 25, 2019

Page 2

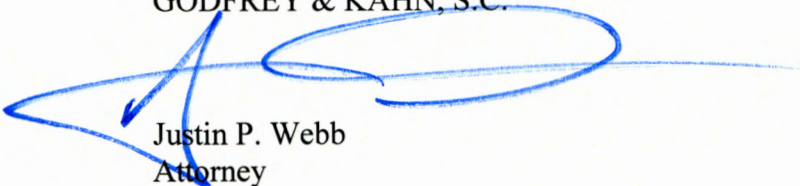
WHCLIP will be notifying approximately three (3) New Hampshire residents and will be among those receiving twelve (12) months of free credit monitoring. WHCLIP will also provide a dedicated call center that potentially affected individuals may call with questions regarding the incident.

In an effort to ensure a similar incident does not occur in the future, WMMS is reviewing the information required by the Plan's accountants and auditors, and reviewing other vendor security practices and procedures. In addition, as noted above, WHCLIP no longer has a relationship with the independent auditor whose credentials were used to accomplish the attack. WHCLIP also intends to work with WMMS and its consultants to identify additional measures to mitigate future attacks and threats.

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

Very truly yours,

GODFREY & KAHN, S.C.



Justin P. Webb
Attorney

JPW

EXHIBIT A

Sample Customer Notification Letter



**Wisconsin
Health Care Liability
Insurance Plan**

Wisconsin Health Care Liability Insurance Plan
PO Box 7873
Madison, WI 53707

<<Mail ID>>
<<Name1>>
<<Address1>>
<<Address2>>
<<Address3>>
<<City>>, <<ST>> <<ZIP>>
<<Country>>

<<Date>>

NOTICE OF DATA BREACH

Dear <<Name>>:

This letter is a follow-up to the letter you previously were sent on December 20th, 2018, from the Wisconsin Health Care Liability Insurance Plan ("WHCLIP," or the "Plan") informing you about a security incident involving the unauthorized acquisition of your personal information. We are contacting you again to provide additional details about the nature of the security incident, and to provide you with twelve (12) months of free credit monitoring services. We are providing you this follow-up notice and offering credit monitoring services because WHCLIP values the security and privacy of your personal information, is committed to ensuring you understand what happened, and to providing you with the tools to assist you with securing and protecting your personal information if you have ongoing concerns.

WHAT HAPPENED?

On December 5, 2018, WHCLIP's accountants advised WHCLIP that an unauthorized third party gained access to a secure file sharing system (Citrix Sharefile) used by the company's accountants for WHCLIP to share financial information required to perform the company's accounting operations as well as statutorily required audits of the Plan. The file sharing system that was accessed without authorization contained information specifically intended for WHCLIP's auditor.

WHCLIP was informed that the unauthorized access occurred on November 4, 2018, and was perpetrated by an attacker using the login credentials of the independent auditor retained to do the yearly required audit of the Plan's financial and attendant operations. Unfortunately, in addition to accessing the secure file sharing system without authorization, the attacker also downloaded files containing names, addresses, and Social Security numbers. Upon learning of the incident, WHCLIP sent out the initial notification you previously received, consistent with Wisconsin law, to ensure that you were aware of the incident without delay.

To be clear, there was no compromise or breach of WHCLIP's systems or networks, or the systems or networks of Wausau MedMal Management, LLC, WHCLIP's Plan Manager.

WHAT INFORMATION WAS INVOLVED?

The personally identifiable information potentially involved includes your name, address, Social Security number, and, in some instances, a Tax Identification Number ("TIN").

WHAT WE ARE DOING

To start, the independent auditor's access to the secure file sharing system has been terminated and the Plan no longer has a relationship with the firm. In addition to fully investigating this incident, WHCLIP is taking measures designed to ensure a similar incident does not occur in the future, including reviewing the information required by our accountants, auditors, and reviewing all our other vendor security practices and procedures. To help relieve concerns and restore confidence following this incident, we have arranged for you to enroll, **at no cost to you**, in an online credit monitoring service *myTrueIdentity* for one year provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies.

Complimentary Credit Monitoring Service

To enroll in this service, go to the *myTrueIdentity* website at www.mytrueidentity.com and in the space "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 at **1-855-288-5422**. When prompted, enter the following 6-digit telephone pass code **<<Insert static 6-digit Telephone Pass Code>>** and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or 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 either do not have a credit file with TransUnion, or who do not have 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, changes of address, and more. The service also includes access to an identity restoration program that provides assistance in restoring your identity in the event that your identity is compromised, as well as up to \$1,000,000 in identity theft insurance with no deductible (policy limitations and exclusions may apply).

WHAT YOU CAN DO

In addition to signing up for *myTrueIdentity*, we encourage you to review the information below for ways to further protect your identity.

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 for the next 12 – 24 months. 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, including your state attorney general and the Federal Trade Commission (FTC). You have the right to obtain a police report if you are a victim of identity theft.

To file a complaint with the FTC, go to <http://www.IdentityTheft.gov> or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

Obtain and Monitor Your Credit Report

We recommend that you 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 access the request form at <https://www.annualcreditreport.com/requestReport/requestForm.action>. Or you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

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

Experian
(888) 397-3742
www.experian.com
P.O. Box 4500
Allen, TX 75013

TransUnion
(800) 888-4213
www.transunion.com
2 Baldwin Place
P.O. Box 1000
Chester, PA 19016

Consider Placing a Fraud Alert on Your Credit Report

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 at least 90 days. 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>.

Take Advantage of Additional Free Resources on Identity Theft

You can further educate yourself regarding identity theft, security freezes, fraud alerts, and the steps you can take to protect yourself against identity theft and fraud by contacting the Federal Trade Commission or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; <http://www.IdentityTheft.gov>; 1-877-ID THEFT (1-877-438-4338); and TTY: 1-866-653-4261. A copy of Taking Charge: What to Do if Your Identity is Stolen, a comprehensive guide from the FTC to help you guard against and deal with identity theft, can be found on the FTC's website at <https://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf>.

The Federal Trade Commission encourages those who discover that their information has been misused to file a complaint with them. Instances of known or suspected identity theft should be promptly reported to law enforcement, the Federal Trade Commission, and your state Attorney General.

Consider a Security Freeze on Your Credit File

You can request a "Security Freeze" on your credit file by sending a request in writing, by mail, to each of the three nationwide credit reporting companies. When a Security Freeze is added to your credit report, all third parties, such as credit lenders or other companies whose use is not exempt under law, will not be able to access your credit report without consent. The Security Freeze may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make that involves access to your credit report. This may include, but is not limited to, new loans, credit, mortgages, insurance, rental housing, employment, investments, licenses, cellular phone service, utility service, digital signature service, Internet credit card transactions, and extension of credit at point of sale. As of September 21, 2018, placing or removing a credit freeze is free.

To place a Security Freeze on your credit files at all three nationwide credit reporting companies, write to the addresses below and include the following information:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
<https://www.freeze.equifax.com>
1-800-685-1111

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
<http://experian.com/freeze>
1-888-397-3742

TransUnion Security Freeze
P.O. Box 2000
Chester, PA 19016
<http://transunion.com/freeze>
1-888-909-8872

1. Your name (first, middle, last including applicable generation, such as JR., SR., II, III, etc.)
2. Your Social Security Number
3. Your date of birth (month, day, and year)
4. Your complete address including proof of current address, such as a current utility bill, bank or insurance statement, or telephone bill
5. If you have moved in the past 2 years, give your previous addresses where you have lived for the past 2 years
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. Include applicable fee. Call or visit each of the credit reporting company websites listed above for information on fees or Security Freeze services. Forms of payment are check, money order, or credit card, or a copy of a valid identity theft report, or other valid report from a law enforcement agency to show you are the victim of identity theft and are eligible for free Security Freeze Services.

Within five business days of receiving your request for a security freeze, the consumer credit reporting company will provide you with a personal identification number (PIN) or password to use if you choose to remove the freeze on your consumer credit report or to authorize the release of your consumer credit report to a specific party or for a specified period of time after the freeze is in place.

For New Mexico Residents: You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have the right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

ADDITIONAL INFORMATION

For Maryland Residents: Maryland residents may also wish to review information provided by the Maryland Attorney General on how to avoid identity theft at <http://www.oag.state.md.us/idtheft>, by sending an email to idtheft@oag.statemd.us, or by calling 410-576-6491.

For North Carolina Residents: North Carolina residents may wish to review information provided by the North Carolina Attorney General at <http://www.ncdoj.gov/Help-for-Victims/ID-Theft-Victims.aspx>, by calling 877-566-7226, or writing to 9001 Mail Service Center, Raleigh, NC 27699.

For California and Wyoming Residents: This notice has not been delayed as a result of a law enforcement investigation.

For Iowa Residents: Iowa residents may report any suspected identity theft to law enforcement or to the Iowa Attorney General, Consumer Protection Division, 1305 E. Walnut St., Des Moines, IA 50319, Telephone: 1-888-777-4590.

For Oregon Residents: Oregon residents may report any suspected identity theft to the Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.

FOR MORE INFORMATION

WHCLIP sincerely apologizes for any inconvenience and concern this incident may cause you. If you have additional questions, please contact us at [insert hotline #], Monday through Friday, 6:00 a.m. to 6:00 p.m. PST.

Sincerely,

Stan Hoffert
Wausau MedMal Management Services, Plan Administrator
Wisconsin Health Care Liability Insurance Plan