STATE OF NH
DEPT OF JUSTICE
2017 FEB -1 AM 9:32

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

January 31, 2017

VIA OVERNIGHT DELIVERY

Attorney General Joseph Foster
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Incident Notification

Dear Attorney General Foster:

On behalf of our client Tufts Health Public Plans, Inc. (formerly Network Health, Inc.), we are writing to inform you of an incident involving our client's reinsurance carrier, Summit Reinsurance Services, Inc. ("Summit"). In the past, Summit provided reinsurance services for Tufts Health Public Plans, Inc. (formerly Network Health, Inc.).

On December 2, 2016, Tufts Health Public Plans, Inc. (formerly Network Health, Inc.) learned from Summit that Tufts Health Public Plans, Inc. (formerly Network Health, Inc.) member data was on a server that had been infected with ransomware. Summit discovered the incident on August 8, 2016. Summit informed Tufts Health Public Plans, Inc. (formerly Network Health, Inc.) that it immediately launched an investigation to determine the nature and scope of this incident and to prevent the further encryption of data contained on the server. Summit also began working with third-party forensic investigators to assist with these efforts. It appears that the unauthorized access to the server first occurred on or around March 13, 2016. Summit has indicated that, to date, it has no direct evidence that such data has been used inappropriately.

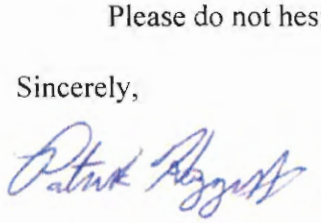
The information contained on the affected server may have included the name, Social Security number, health insurance information, provider's name, and/or claim-focused medical records containing diagnosis and clinical information for certain Tufts Health Public Plans, Inc. (formerly Network Health, Inc.) members. This information was provided to Summit so that it could provide reinsurance services.

On January 31, 2017, Summit mailed a notification letter to one New Hampshire resident. The notice contains information and access to resources that potentially affected individuals may use to better protect against the possible misuse of their information. The notice was provided in substantially the same form as the letter attached hereto. Summit is offering potentially affected individuals access to one year of free credit monitoring and identity restoration services through Experian. Summit also is providing a call center for affected individuals to call with any questions.

Tufts Health Public Plans, Inc. (formerly Network Health, Inc.) believes that it is appropriate for Summit to notify potentially affected New Hampshire residents. Under New Hampshire law, the notification obligations related to the incident at Summit are those of the owner or licensor of the computerized data. N.H. REV. STAT. ANN. § 359-C:20(I)(a). The notification obligation regarding the data would belong to Tufts Health Public Plans, Inc. (formerly Network Health, Inc.) only if Summit maintained o the information on behalf of Tufts Health Public Plans, Inc. (formerly Network Health, Inc.). *See id.* at § 359-C:20(I)(c). Summit does not store the data on Tufts Health Public Plans, Inc.'s (formerly Network Health, Inc.'s) behalf; rather, Summit stores the data to determine its own underwriting, reinsurance and claims-payment obligations. This comports with the HIPAA reinsurance exception that specifically states that each entity acts on its own behalf when the health plan purchases reinsurance or stop loss insurance, when the health plan submits a claim to the reinsurer or stop loss carrier, and when the reinsurer or stop loss carrier pays the claim. *See* http://www.hhs.gov/hipaa/for-professionals/faq/255/is-reinsurer-businees-associate-of-health-plan/index.html. Consequently, we believe that Summit has the duty under New Hampshire law to notify New Hampshire residents and your office. Nevertheless, we are voluntarily reporting the incident to your office.[1] By submitting this report, Tufts Health Public Plans, Inc. (formerly Network Health, Inc.) is not acquiescing that it is the data owner or licensor and reserves all of its rights.

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

Sincerely,



Patrick H. Haggerty
Partner

Enclosure

[1] This report is not, and does not constitute, a waiver of personal jurisdiction.

SummitRe

7030 Pointe Inverness Way
Suite 350
Fort Wayne, IN 46804

STATE OF IN
DEPT OF JUSTICE
2017 FEB -1 AM 9:32

TO THE PARENT OR GUARDIAN OF
FIRST NAME MI LAST NAME
ADDRESS1
ADDRESS2
CITY STATE ZIP

January 31, 2017

Re: Notice of Data Security Incident

Dear Parent or Guardian of First Name MI Last Name:

Summit Reinsurance Services, Inc. ("Summit") is writing to inform you of a data security event that may affect the security of your dependent's personal information and to provide you with information on how to better protect against the possible misuse of your dependent's information. Summit has your dependent's information because we provide underwriting and reinsurance services to certain insurance companies and self-funded employer groups. In your dependent's case, we worked with Tufts Health Public Plans, Inc. (formerly Network Health, Inc.). This incident occurred at Summit. Tufts Health Public Plans, Inc. (formerly Network Health, Inc.)'s system was not affected by this incident.

What Happened? On August 8, 2016, Summit discovered that ransomware had infected a server containing certain personal information. Summit immediately launched an investigation to determine the nature and scope of this event and to prevent the encryption of data contained on the server. Summit also began working with third-party forensic investigators to assist with these efforts. Based on the forensic investigation, it appears that the unauthorized access to the server first occurred on March 13, 2016. To date, Summit has no direct evidence that such data has been used inappropriately.

What Information Was Involved? The information contained on the affected server may have included your dependent's name, Social Security number, health insurance information, provider's name, and/or claim-focused medical records containing diagnosis and clinical information.

What Are We Doing? We take the security of information in our care very seriously. Although the forensic investigation is ongoing, to date, we have found no direct evidence of actual or attempted misuse of personal information on the affected server as a result of this incident. Nevertheless, in an abundance of caution, we are notifying you of this incident. Additionally, we have notified your dependent's insurance company.

We are also providing you with information you can use to better protect against identity theft and fraud, as well as access to one year of identity theft protection and restoration services for your dependent at no cost to you. You can find more information and steps you can take, as well as information on how to enroll in the identity theft protection services, in the enclosed *Steps You Can Take to Prevent Identity Theft and Fraud.*

We are committed to the security of the information in our system and we have worked, and will continue to work, to enhance the protections in place to protect data in our care.

What Can You Do? You can review the enclosed *Steps You Can Take to Prevent Identity Theft and Fraud* for more information on ways to protect against the potential misuse of your dependent's information. You can also enroll to receive the identity theft protection and restoration services we are offering your dependent at no cost.

For More Information. Again, we take the security of sensitive information in our care very seriously and we regret any concern or inconvenience this incident may cause you. We understand you may have questions that are not addressed in this notice. If you have additional questions, please call our dedicated assistance line at (877) 215-9747, Monday through Friday, 9 a.m. to 7 p.m. EST (closed on U.S. observed holidays) and provide Reference Number 2996113016 when calling.

Sincerely,

Mark Troutman

Mark
Troutman
President

STEPS YOU CAN TAKE TO PREVENT IDENTITY THEFT AND FRAUD

To help you further safeguard against any potential misuse of your dependent's personal information, we are offering access to one (1) year of **complimentary** membership in Experian's® Family Secure®. Family Secure monitors your Experian credit report to notify you of key changes. In addition, Family Secure will tell you if the minor has a credit report, a potential sign that his or her identity has been stolen.

Activate Family Secure Now in Three Easy Steps

1. **ENSURE That You Enroll By: April 30, 2017** (Your code will not work after this date.)
2. **VISIT the Family Secure Web Site to enroll: www.familysecure.com/enroll**
3. **PROVIDE Your Activation Code: [code]**

If you have questions or need an alternative to enrolling online, please call **(888) 276-0529** and provide engagement #: **PC105332.** A credit card is not required for enrollment. Once activated, your dependent's Family Secure membership includes the following features:

- **Monthly monitoring** to determine whether enrolled minors in your household have an Experian credit report
- **Alerts of key changes** to your children's Experian credit report
- **Identity Theft Resolution assistance**: Toll-free access to US-based customer care and a dedicated Identity Theft Resolution agent who will walk you through the process of fraud resolution from start to finish for seamless service. They will investigate each incident; help with contacting credit grantors to dispute charges and close accounts including credit, debit and medical insurance cards; assist with freezing credit files; contact government agencies.
- **$2,000,000 Product Guarantee**[1]

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your dependent's account statements, to monitor your dependent's credit report to ensure credit has not been granted in his or her name, and to monitor explanation of benefits forms for suspicious activity. While minors do not have credit files, the following information relates to protecting one's credit once established:

Under U.S. law, adults with credit files are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of a credit report. At no charge, you can also have these credit bureaus place a "fraud alert" on a credit file that alerts creditors to take additional steps to verify identity prior to granting credit in your dependent's name. Note, however, that because it tells creditors to follow certain procedures to protect identity, it may also delay one's ability to obtain credit while the agency verifies identity. As soon as one credit bureau confirms the fraud alert, the others are notified to place fraud alerts on the credit file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.

Equifax	Experian	TransUnion
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022-2000
800-525-6285	888-397-3742	800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

[1] The Family Secure Product Guarantee is not available for Individuals who are residents of the state of New York.

You may also place a security freeze on credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised that placing a security freeze on a credit report may delay, interfere with, or prevent the timely approval of any requests made for new loans, credit mortgages, employment, housing, or other services. If a consumer has been a victim of identity theft, and provides the credit bureau with a valid police report, the bureau cannot charge the consumer to place, lift or remove a security freeze. In all other cases, a credit bureau may charge a fee to place, temporarily lift, or permanently remove a security freeze. Consumer must place a security freeze separately with each of the three major credit bureaus listed above in order to place a freeze on all credit files. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348 1-800-685-1111 www.equifax.com/help/credit-freeze/en_cp	Experian Security Freeze P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/center.html	TransUnion PO Box 2000 Chester, PA 19022-2000 1-888-909-8872 www.transunion.com/securityfreeze

In order to request a security freeze, the following information is required: full name, address, date of birth, Social Security number, current address, all addresses for up to five previous years, email address, a copy of state identification card or driver's license, and a copy of a utility bill, bank or insurance statement, or other statement proving residence. Fees vary based on state of residence, but commonly range from $5 to $10.

You can further educate yourself regarding identity theft, fraud alerts, and the steps you can take to protect the misuse of personal information 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, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Instances of known or suspected identity theft should also be reported to law enforcement or your state Attorney General. The mailing of this notice was not delayed by law enforcement.