Taft/

40 North Main Street, Suite 1700
Dayton, OH 45423-1029
Tel: 937.228.2838 | Fax: 937.228.2816
taftlaw.com

SCOT GANOW
937.641.2041
sganow@taftlaw.com

RECEIVED
AUG 03 2022
CONSUMER PROTECTION

August 2, 2022

VIA FEDERAL EXPRESS

CONFIDENTIAL

Attorney General John M. Formella
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

RE: CareSource

To Whom It May Concern:

In accordance with New Hampshire Revised Code §359-C:19, et. seq., I am providing the following notice of a security incident on behalf of our client, CareSource ("CareSource").

Name and Contact Information of Person Reporting the Security Incident.

Scot Ganow, Esq., CIPP/US
Outside Counsel to CareSource
Taft Stettinius & Hollister LLP
40 North Main Street, Suite 1700
Dayton, Ohio 45423
937-641-2041
sganow@taftlaw.com

Name and address of the owner of the data affected and the business that experienced the security incident, and the type of business.

Business that Owns the Affected Data:

CareSource
230 North Main Street
Dayton OH 45402
CareSource offers insurance services to its members.

Business that Experienced the Security Incident:

OneTouchPoint, Inc.
1225 Walnut Ridge Drive
Hartland, Wisconsin 53029.
Attention: Incident Response
OneTouchPoint is a service provider that provides marketing services for CareSource.

Brief Description of Incident. CareSource contracts with OneTouchPoint ("OTP") for the purposes of mailing newsletters and health care educational materials to CareSource members. On April 29, 2022, OTP reported to CareSource that it had experienced a ransomware attack on April 27, 2022, targeting OTP's systems, which potentially contained OTP and customer data, including some CareSource member information. OTP initially reported that it believed only OTP data was affected. At that time, OTP took its systems offline to assess impact and begin remediation efforts. CareSource immediately terminated its connections to OTP resources when it learned of the incident. **At no time was there any impact to CareSource systems.**

After a formal investigation, OTP confirmed to CareSource on June 3, 2022, that CareSource files were among the files encrypted by the attacker. However, OTP indicated that only OTP's data was exfiltrated, and OTP had no information showing that CareSource member data had been viewed or removed from OTP systems, although OTP could not be absolutely sure. CareSource systems were not affected by this incident and OTP has no information that CareSource member information was viewed or removed from its systems.

CareSource is providing notice to individuals whose information was contained in OTP's systems after OTP completed its internal investigation of the incident, after the potentially impacted data files were properly reviewed to ascertain the individuals that required notice under applicable law, and after applicable state regulators reviewed and approved the individual notice letter as required by CareSource's contracts with those regulators. As the data was still encrypted by the threat actor, CareSource is providing individual notices in accordance with the Health Insurance Portability and Accountability Act (HIPAA) and is providing media and substitute notice in jurisdictions where required by HIPAA.

Information Compromised. According to the investigation, personal information that may have been impacted includes:

- Name
- Address
- Member ID
- Age
- Gender
- Immunizations
- Plan name
- Allergies
- Health screenings
- Vital signs
- Diagnosis
- Medication

Company Response. OTP reported that it disconnected and rebuilt its systems to ensure the threat actor was no longer in the systems environment. OTP hired a third-party forensic firm to assist in the recovery of the network and determine the root cause. OTP also reported that it implemented

additional technical controls including but not limited to new endpoint protection, detection software and rolling password reset cycle.

Once aware of the impact to CareSource member information, CareSource began its own investigation and commenced its incident response planning. Such work included working with OTP to understand the scope of the incident, identifying the CareSource member information impacted and determining notice requirements. CareSource is no longer utilizing OTP for mailing of member materials. As with any security incident, CareSource will work with its vendors to properly investigate and review any practices that can be improved to prevent a recurrence of an incident like this.

Number of Affected Individuals in New Hampshire. The investigation confirmed that 25 New Hampshire residents may have been affected by the incident. In the event CareSource determines any additional New Hampshire residents are impacted, CareSource shall update this notice accordingly.

Notice to Affected Individuals. An electronic copy of the notice to the affected individuals is attached. CareSource has provided individual notice letters to OTP for OTP to send on CareSource's behalf with the expectation that notices will be sent the week of August 1, 2022, or as soon as reasonably possible.

Credit Monitoring Services. Because the personal information potentially at risk as a result of the incident did not include social security numbers or other financial information, neither CareSource nor OTP are providing credit monitoring services.

Notice Letter Template

OneTouchPoint

<Date>
<Parent or Guardian of>
<FirstName> <MiddleInitial> <LastName>
<Address1>
<Address2>
<City>, <State> <ZIP>

RE: Notice of Security Breach

Dear <Parent or Guardian of><FirstName><LastName>

OneTouchPoint ("OTP") prints and mails newsletters for CareSource® and has files with some of your information. This letter is notice of a cybersecurity incident at OTP that may have improperly disclosed your information.

What Happened
On April 28, 2022, OTP learned of an attack on its systems. OTP found out that some files that had your info in them were locked by the attacker and could not be opened. OTP did not find that your info had been viewed or removed from its systems but cannot be sure.

What Information Was Involved
Your Social Security number and other financial information was not in the files and was not impacted. The personal info that was at risk includes:

- Name
- Address
- Member ID
- Age
- Gender
- Vital Signs
- Diagnosis
- Medications
- Allergies
- Health Screenings
- Immunizations
- Plan Name

What We Are Doing
OTP shut down its systems to prevent further problems. It rebuilt its systems to make sure all issues were fixed. OTP also made its systems safer by adding additional technical controls.

What You Can Do
We do not believe your info is in danger of misuse. Still, you should always review your mail from CareSource to make sure it looks right. Let CareSource know of any concerns.
Please call us if you have any questions about this notice at **877-237-3894,** (TTY: 711) Monday – Friday, 8:00 a.m. to 8:00 p.m. Central Time.

Sincerely,
[Name and Title]

H8452_OH-MYC-M-1444502

ODM Approved: 7/27/2022