breezeline™

October 11, 2022

CONFIDENTIAL
VIA OVERNIGHT DELIVERY

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

Re: Notice of Data Security Incident

To the Secretary of the New Hampshire Attorney General:

I am writing on behalf of Cogeco US Finance, LLC, d/b/a Breezeline (f/k/a Atlantic Broadband) to notify you of a data security incident involving Conifer Value-Based Care, LLC ("Conifer"), a subcontractor and service provider that provides services to vendors which assist health plans and employers, including Cogeco US Finance, LLC, d/b/a Breezeline ("Health Plan"). A copy of the notification being sent by Conifer to 176 New Hampshire residents on October 11, 2022 by first class mail in accordance with notification requirements under state law is attached to this letter.

On March 21, 2022, Conifer discovered that an unauthorized third party gained access to certain Microsoft Office 365-hosted business email accounts through phishing. We were informed by Conifer that, upon discovery, Conifer immediately took action to prevent any further unauthorized activity, began an investigation, and engaged a leading security firm. Based on the investigation, the unauthorized party was able to access certain Conifer Value-Based Care business email accounts between March 17, 2022 and March 22, 2022. We were informed that those email accounts are separate from Conifer's internal network and systems, which were not affected by this incident.

We were informed that based on the investigation and a detailed review that was performed and ultimately completed on June 22, 2022, it was determined that personal information associated with Conifer's client StrateBEN ("Client") (which provides services to the Health Plan) was in the impacted business email account. We understand that Conifer notified Client of the incident on June 24, 2022. We were informed that additional data enrichment and validation was further conducted to confirm the impacted individuals and impacted health plans with which such individuals were associated. Client confirmed that personal information associated with the Health Plan was in one of the impacted accounts. Client therefore notified the Health Plan of the incident on August 26, 2022.

Personal information involved in this incident may have included: full name, home address, date of birth, Social Security number, health insurance subscriber number, medical information (such as diagnosis and treatment information), and billing and claims information. Please note that not all data elements were involved for all individuals.

breezeline™

Conifer informed us that when it discovered the incident, Conifer immediately took action to prevent any further unauthorized activity, including resetting the user password for the business email accounts where unauthorized activity was detected and blocking malicious IP addresses and URLs. Conifer also informed us that it has and continues to enhance its security controls and monitoring practices as appropriate to minimize the risk of any similar incident in the future, and Conifer accelerated its implementation of multi-factor authentication for all business email accounts within the environment, which is complete.

Free credit monitoring services for 24 months are being offered to all impacted New Hampshire residents.

If you have any questions regarding this incident or if you desire further information or assistance, please email me at lbrown@breezeline.com or call my direct line at 978-604-4581.

Sincerely,

Leslie J. Brown
Senior Vice President and General Counsel

Enclosure

CONIFER
HEALTH SOLUTIONS®
P.O. Box 989728
West Sacramento, CA 95798-9728

To Enroll, Please Call:
1-833-764-2096
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code: <<XXXXXXXX>>

<<First Name>><<Middle Initial>><<Last Name>><<Suffix>>
<<Address 1>>
<<Address 2>>
<<City>><<State>><<Zip>>

October 11, 2022

Su información personal puede haber estado involucrada en un incidente de datos. Si desea recibir una version de esta carta en español, por favor llame 1-833-764-2096.

Notice of Data Breach

To <<First Name>> <<Middle Initial>> <<Last Name>> <<Suffix>>:

We are writing to inform you of a data security incident that impacted Conifer Value-Based Care, LLC ("Conifer" or "we"), a subcontractor and service provider that provides services to vendors which assist health plans and employers, including <<Variable Text 1: Provider Name >> ("Health Plan") with which you are, were, or may have been affiliated. This incident may have affected your personal information.

What happened?

On March 21, 2022, Conifer discovered that an unauthorized third party gained access to certain Microsoft Office 365-hosted business email accounts through phishing. "Phishing" occurs when an email is sent that looks like it is from a trustworthy source, but it is not. The phishing email prompts the recipient to share or give access to certain information. Upon discovery, Conifer immediately took action to prevent any further unauthorized activity, began an investigation, and engaged a leading security firm.

Based on the investigation, the unauthorized party was able to access certain Conifer Value-Based Care business email accounts between March 17, 2022 and March 22, 2022. Those email accounts are separate from Conifer's internal network and systems, which were not affected by this incident. As further detailed below, Conifer determined that your personal information was in one of the impacted business email accounts.

After identifying the business email accounts that were accessed, Conifer performed data enrichment and validation in order to identify potentially impacted individuals and Conifer was able to associate its client, StrateBEN ("Client") (which provides services to the Health Plan) with some of the potentially impacted individuals. Conifer therefore notified Client of the incident on June 24, 2022.

After notifying Client, additional data enrichment and validation was conducted to further confirm impacted individuals and the impacted entities with which such individuals were associated. This assessment confirmed that as a recipient of Conifer services, the Health Plan was an impacted entity and that your personal information (as a current or former Health Plan member) was in one of the impacted Conifer business email accounts. Client therefore notified the Health Plan of the incident on August 26, 2022.

What information may have been involved?

Personal information involved in this incident may have included one or more of the following elements: full name, home address, date of birth, health insurance information, and medical information (such as medical record number, provider and

facility, and/or diagnosis and treatment information). Please note that not all data elements were involved for all individuals. Our review also indicates that your Social Security number was also included in the affected data.

What Conifer is doing.

Conifer takes privacy and security very seriously. As soon as Conifer discovered the incident, Conifer immediately took action to prevent any further unauthorized activity, including resetting the user password for the business email accounts where unauthorized activity was detected and blocking malicious IP addresses and URLs. Conifer has and continues to enhance its security controls and monitoring practices as appropriate to minimize the risk of any similar incident in the future, and Conifer accelerated its implementation of multi-factor authentication for all business email accounts within the environment, which is complete.

In addition, Conifer has arranged to offer you credit monitoring and identity restoration services for a period of <<12/24>> months, at no cost to you. You have until January 11, 2023 to activate these services, and instructions on how to activate these services are included in the enclosed Reference Guide.

What you can do.

In addition to enrolling in complimentary credit monitoring, the enclosed Reference Guide includes additional information on general steps you can take to monitor and protect your personal information. Conifer encourages you to carefully review credit reports and statements sent from providers as well as your insurance company to ensure that all account activity is valid. Any questionable charges should be promptly reported to the company with which you maintain the account.

For more information

If you have any questions about this matter or would like additional information, please refer to the enclosed Reference Guide or call toll-free 1-833-764-2096. This call center is open from 9 am – 9 pm Eastern Time, Monday through Friday, except holidays.

<<Variable Text 2>>

Conifer sincerely regrets that this incident occurred and apologizes for any inconvenience this incident may have caused you.

Sincerely,

Zanib Arshed
Conifer Privacy Office

Reference Guide

Review Your Account Statements

Carefully review statements sent to you from your healthcare providers, insurance company, and financial institutions to ensure that all of your account activity is valid. Report any questionable charges promptly to the company with which you maintain the account.

Provide Any Updated Personal Information to Your Health Care Provider

Your health care provider's office may ask to see a photo ID to verify your identity. Please bring a photo ID with you to every appointment if possible. Your provider's office may also ask you to confirm your date of birth, address, telephone, and other pertinent information so that they can make sure that all of your information is up-to-date. Please be sure and tell your provider's office when there are any changes to your information. Carefully reviewing this information with your provider's office at each visit can help to avoid problems and to address them quickly should there be any discrepancies.

Order Your Free Credit Report

To order your free annual credit report, visit www.annualcreditreport.com, call toll-free at (877) 322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three credit bureaus provide free annual credit reports only through the website, toll-free number or request form.

Upon receiving your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you have not requested credit. Some companies bill under names other than their store or commercial names; the credit bureau will be able to tell if this is the case. Look in the "personal information" section for any inaccuracies in information (such as home address and Social Security Number).

If you see anything you do not understand, call the credit bureau at the telephone number on the report. Errors may be a warning sign of possible identity theft. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing. Information that cannot be explained should also be reported to your local police or sheriff's office because it may signal criminal activity.

How to Enroll in IDX Credit and Identity Monitoring Services

As a safeguard, you may enroll, at no cost to you, in an online credit monitoring and identity restoration service provided by IDX.

To enroll in this service, please call 1-833-764-2096 or visit https://app.idx.us/account-creation/protect and follow the instructions for enrollment using the Enrollment Code provided above.

The monitoring included in the membership must be activated to be effective. You have until January 9, 2023 to enroll in these services. Please note that credit monitoring services may not be available for individuals who have not established credit 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. If you need assistance, IDX will be able to assist you.

We encourage you to take advantage of these protections and remain vigilant for incidents of potential fraud and identity theft, including regularly reviewing and monitoring your credit reports and account statements.

Contact the U.S. Federal Trade Commission

If you detect any unauthorized transactions in any of your financial accounts, promptly notify the appropriate payment card company or financial institution. If you detect any incidents of identity theft or fraud, promptly report the matter to your local law enforcement authorities, state Attorney General and the FTC.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft by using the contact information below:

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

Place a Fraud Alert on Your Credit File

To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect against the possibility of an identity thief opening new credit accounts in your name. When a credit grantor checks the credit history of someone applying for credit, the credit grantor gets a notice that the applicant may be the victim of identity theft. The alert notifies the credit grantor to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free fraud numbers provided below. You will reach an automated telephone system that allows flagging of your file with a fraud alert at all three credit bureaus.

Equifax	P.O. Box 105069 Atlanta, Georgia 30348	1- 888-766-0008	www.equifax.com
Experian	P.O. Box 9554 Allen, Texas 75013	1-888-397-3742	www.experian.com
TransUnion	P.O. Box 2000 Chester, PA 19016	1-800-680-7289	www.transunion.com

Security Freezes

You have the right to request a credit freeze from a consumer reporting agency, free of charge, 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 security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security 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 security freeze may delay your ability to obtain credit.

Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit bureau. To place a security freeze on your credit report you must contact the credit reporting agency by phone, mail, or secure electronic means and provide proper identification of your identity. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue.

Below, please find relevant contact information for the three consumer reporting agencies:

Equifax Security Freeze	P.O. Box 105788 Atlanta, GA 30348	1-800-685-1111	www.equifax.com
Experian Security Freeze	P.O. Box 9554 Allen, TX 75013	1-888-397-3742	www.experian.com

TransUnion	P.O. Box 160 Woodlyn, PA 19094	1-888-909-8872	www.transunion.com

Once you have submitted your request, the credit reporting agency must place the security freeze no later than 1 business day after receiving a request by phone or secure electronic means, and no later than 3 business days after receiving a request by mail. No later than five business days after placing the security freeze, the credit reporting agency will send you confirmation and information on how you can remove the freeze in the future.

For Residents of Massachusetts

You have the right to obtain a police report with respect to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For Residents of North Carolina

You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-919-716-6000, www.ncdoj.gov.