MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

Gregory J. Bautista
Office: (267) 930-1509
Fax: (267) 930-4771
Email: gbautista@mullen.law

1127 High Ridge Road, #301
Stamford, CT 06905

May 28, 2021

VIA U.S. MAIL

Consumer Protection Bureau
Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Event

Dear Sir or Madam:

We represent Caravus LLC ("Caravus") located at 168 N. Meramec Avenue, Suite 300, St. Louis, MO, 63105, and are writing to notify your office of an incident that may affect the security of some personal information relating to twenty (20) New Hampshire residents. This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Caravus does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

In November 2020, Netgain Technology, LLC ("Netgain"), a third-party provider based in St. Cloud, MN that offers information technology network and computer systems to organizations like Caravus, reported that it experienced a ransomware incident that resulted in encryption of certain Netgain systems. Netgain reported the incident to law enforcement and worked with forensic investigators to investigate. Following its investigation, Netgain notified its customers that an unknown actor may have accessed or acquired certain customer data. Caravus was formally informed that its data was *not* impacted by this incident.

In 2015, Netgain oversaw a migration of Caravus data to a new server. However, Caravus recently learned Netgain failed to destroy some legacy Caravus data on the old server following this migration. Caravus began a thorough and lengthy investigation to determine what information remained following the server migration and potentially impacted by the ransomware event. Based

on Caravus's investigation, it was determined on April 26, 2021, that this incident may have involved some personal information that Caravus received from its clients in or before 2016.

The information that could have been subject to unauthorized access includes name, and Social Security number.

Notice to New Hampshire Residents

On or about May 28, 2021, Caravus provided written notice of this incident to all affected individuals, which includes twenty (20) New Hampshire residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, Caravus moved quickly to investigate and respond to the incident, and notify potentially affected individuals. Caravus is providing access to credit and identity monitoring services for one (1) year, through IDX, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Caravus is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Caravus is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-1509.

Very truly yours,

Gregory J. Bautista of
MULLEN COUGHLIN LLC

GJB /eyl

EXHIBIT A

caravus
C/O IDX
P.O. Box 989728
West Sacramento, CA 95798-9728

To Enroll, Please Call:
(833) 664-2019
Or Visit:

https://response.idx.us/protectcaravus

Enrollment Code: <<enrollment>>

<<FIRST NAME>> <<LAST NAME>>
<<ADDRESS1>>
<<ADDRESS2>>
<<CITY>>, <<STATE>> <<ZIP>>

May 28, 2021

<<VAR 3 HEADER>>

Dear <<FIRST NAME>> <<LAST NAME>>:

Caravus, LLC ("Caravus") is an independent health care insurance broker that partners with individuals and employers to secure health plan coverage. The privacy and security of the personal information we maintain on behalf of our clients' employees is of the utmost importance to Caravus. As a partner to your current or former employer, and out of an abundance of caution, we are writing with important information regarding a data security incident involving a third-party cloud services provider. Although we have no evidence of actual or attempted misuse of your information, we want to provide you with information about the incident, our response, and resources available to you to help protect your personal information from possible misuse, should you feel it is appropriate to do so.

What Happened?

In November 2020, Netgain Technology, LLC ("Netgain"), a third-party provider based in St. Cloud, MN that offers information technology network and computer systems to organizations like Caravus, reported that it experienced a ransomware incident that resulted in encryption of certain Netgain systems. Netgain reported the incident to law enforcement and worked with forensic investigators to investigate. Following its investigation, Netgain notified its customers that an unknown actor may have accessed or acquired certain customer data. Caravus was formally informed that its data was *not* impacted by this incident.

In 2015, Netgain oversaw a migration of Caravus data to a new server. However, Caravus recently learned Netgain failed to destroy some legacy Caravus data on the old server following this migration. We began a thorough and lengthy investigation to determine what information remained following the server migration and potentially impacted by the ransomware event. Based on our investigation, it was determined on April 26, 2021, that this incident may have involved some of your personal information that Caravus had maintained on behalf of your employer in or before 2016.

What Information Was Involved?

Our investigation determined that your name and <<Data Elements>> may have been accessed and/or acquired by an unauthorized individual. Although we are unaware of any actual or attempted misuse of your personal information, we are providing you with this notice out of an abundance of caution.

What We Are Doing.

We take the confidentiality, privacy, and security of information in our possession very seriously. Upon learning of this

incident, Caravus moved quickly to investigate and respond. Caravus is no longer using Netgain as a service provider. Additionally, as part of our ongoing commitment to the privacy of personal information in our care and to protect against incidents like this in the future, Caravus has taken and continues to take steps to further strengthen its policies, procedures and existing security measures, including the security measures in place at its third-party vendors.

As an added precaution, we are offering identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: twelve (12) months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do.

Please review the enclosed *Steps You Can Take to Help Protect Your Information*, which contains information on what you can do to better protect against possible misuse of your information. We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. You will also find information on how to enroll in the credit monitoring services offered.

For More Information.

We regret that this occurred and understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at (833) 664-2019, Monday through Friday from 8:00 am – 8:00 pm Central Time.

Sincerely,

J.J. Flotken
Managing Partner

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

We encourage you to contact IDX with any questions and to enroll in free identity protection services by calling (833) 664-2019 or going to https://response.idx.us/protectcaravus and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 8:00 am – 8:00 pm Central Time. Please note the deadline to enroll is August 28, 2021.

1. Website and Enrollment. Go to https://response.idx.us/protectcaravus and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at (833) 664-2019 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and 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. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street NW, Washington, D.C. 20001; 202-727-3400; and oag@dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us. Caravus is located at 168 N. Meramac, Suite 300, St. Louis, MO, 63105.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov/.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 6 Rhode Island residents impacted by this incident.