LEWIS BRISBOIS

LEWIS BRISBOIS BISGAARD & SMITH LLP

Alyssa R. Watzman
1700 Lincoln Street, Suite 4000
Denver, Colorado 80203
Alyssa.Watzman@lewisbrisbois.com
Direct: 720.292.2052

December 10, 2021

VIA E-Mail

Attorney General John Formella
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301
E-Mail: DOJ-CPB@doj.nh.gov

Re: Notice of Data Security Incident

Dear Attorney General Formella:

Lewis Brisbois Bisgaard & Smith LLP represents Icon Voice Networks, LLC ("ICON"), an entity located in the state of Texas, in connection with a data security incident described in greater detail below. This letter is being sent because the personal information of certain New Hampshire residents may have been affected by a recent data security incident experienced by Icon. The incident may have involved unauthorized access to the New Hampshire residents' name and Social Security numbers.

On September 27, 2021, ICON discovered that it had experienced an incident disrupting access to certain of its systems. Upon receipt of this information, ICON immediately took steps to secure its environment and engaged independent digital forensics and incident response experts to conduct an investigation to determine what happened and to identify any personal information that may have been accessed or acquired without authorization. As a result of this independent investigation, ICON learned on November 12, 2021 that personal information may have been accessed or acquired from the ICON digital environment, and that such data may have contained personal information belonging to certain New Hampshire residents.

ICON notified one potentially affected New Hampshire resident of this incident via versions of the attached sample letters on December 10, 2021. In so doing, ICON offered notified individuals 12 months of complimentary identity protection services through IDX, a global leader in risk mitigation and response. ICON has also reported this incident to the Federal Bureau of Investigation and is cooperating to aid law enforcement.

Please contact me should you have any questions.

Best regards,

/s/ Alyssa R. Watzman

Alyssa R. Watzman of
LEWIS BRISBOIS BISGAARD &
SMITH LLP

Encl: Sample Consumer Notification Letters

Icon Voice Networks, LLC

10300 SW Greenburg Rd. Suite 570
Portland, OR 97223

To Enroll, Please Call:
1-800-939-4170
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code: <<XXXXXXXX>>

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

December 10, 2021

Subject: Notice of Data Security Incident

Dear <<First Name>> <<Last Name>>,

I am writing to inform you of a data security incident experienced by Icon Voice Networks, LLC ("ICON") that may have affected your personal information. ICON takes the privacy and security of all personal information very seriously. Please read this letter carefully as it contains information regarding the incident and steps that you can take to help protect your personal information.

What Happened? On September 27, 2021, ICON discovered that it had experienced an incident disrupting access to certain of its systems. In response, ICON took immediate steps to secure its systems and launched an investigation. In so doing, ICON engaged independent digital forensics and incident response experts to determine what happened and to identify any personal information that may have been accessed or acquired without authorization as a result. On November 12, 2021, as a result of this investigation, ICON learned that your personal information may have been accessed or acquired without authorization in connection with the incident which is the reason for this notification. Please note that ICON is not aware of the misuse, or attempted misuse, of any potentially impacted information.

What Information Was Involved? The information potentially impacted in connection with this incident included information contained within files associated with your HSA account, 401K, and health insurance coverage, as well as your UNUM beneficiary forms such as your name as well as your <<variable text>>.

What Are We Doing? As soon as ICON discovered this incident, ICON took the steps described above. In addition, ICON implemented measures to enhance the security of its digital environment in an effort to minimize the risk of a similar incident occurring in the future. ICON also notified the Federal Bureau of Investigation of this incident and will provide whatever cooperation is necessary to hold the perpetrator(s) of the incident accountable.

Although ICON has no evidence of the misuse of any potentially impacted information, ICON is providing you with information about steps that you can take to help protect your personal information and is offering you identity theft protection services at no cost through IDX – a data breach and recovery services expert. These services include 12 months of credit monitoring[1] and dark web monitoring, a $1 million identity fraud loss reimbursement policy, and fully managed identity theft recovery services.

The deadline to enroll in these services is March 10, 2022. With this protection, IDX will help to resolve issues if your identity is compromised.

[1] To receive credit monitoring services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

What You Can Do: You can follow the recommendations on the following page to protect your personal information. ICON also encourages you to enroll in the complementary services being offered to you through IDX by using the enrollment code provided above.

For More Information: Further information about how to protect your personal information appears on the following page. If you have questions or need assistance, please call IDX at 1-800-939-4170 from 8 am to 8 pm Central Time, Monday through Friday. Call center representatives are fully versed on this incident and can answer any questions.

Please accept my sincere apologies and know that ICON takes this matter very seriously and deeply regrets any worry or inconvenience that this may cause you.

Sincerely,

Kevin Kelleher, CEO
Icon Voice Networks, LLC

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. 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, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may 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 1-877-322-8228, 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 also can contact one of the following three national credit reporting agencies:

Equifax
P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian
P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: 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 one year. 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.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

New York Attorney General
Bureau of Internet and Technology Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General
150 South Main Street
Providence, RI 02903
http://www.riag.ri.gov
1-401-274-4400

Washington D.C. Attorney General
441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.