COZEN O'CONNOR

May 17, 2023

Lori Kalani
Direct Phone 202-471-3407
Direct Fax 202-618-4825
lkalani@cozen.com

VIA EMAIL (CONSUMER@AG.IOWA.GOV)

Consumer Protection Division
Security Breach Notifications
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, Iowa 50319-0106

Re: Notice of Cybersecurity Incident Relating to Iowa Residents

To Whom it May Concern:

As DISH Network, LLC (DISH) has previously publicly disclosed, the company experienced a cybersecurity incident on February 23 that affected some of its internal servers and IT telephony and involved the extraction of certain data from its IT systems. DISH now understands that the extracted data includes personal information for certain Iowa residents. DISH is not aware of any misuse of this information and has taken steps to confirm that the third party has deleted it. Additional information regarding the incident and DISH's response is included below.

Upon detecting the incident, DISH immediately activated its incident response and business continuity plans designed to contain, assess and remediate the situation. DISH took steps to prevent further access to the impacted systems, including temporarily shutting down its internal network. The services of cybersecurity experts and outside advisors were retained to assist in the evaluation of the situation, and once DISH determined that the outage was due to a cybersecurity incident, it promptly notified appropriate law enforcement authorities. In the following days, DISH further learned and disclosed that certain data had been extracted from its IT systems as part of this incident.

DISH has since determined that its customer databases were not accessed in this incident. However, DISH confirmed that certain employee-related records and personal information (along with information of some former employees, family members and a limited number of other individuals) were among the data extracted.

The process of locating personal information in the extracted dataset and matching that information to individuals so that DISH could notify them, was complex and time-consuming. This work was substantially completed on May 8, 2023. The affected information differs by individual and can include vaccination record, health insurance information, medical information (primarily documentation for time off), financial account number, driver's license or other government ID number, date of birth, and/or payment card number. DISH began notifying these individuals on May 15, 2023. DISH is offering each of these individuals two years of free credit monitoring and protection services from TransUnion.

As noted above, DISH is not aware of any evidence that any personal information was misused as a result of this incident, and it has received confirmation that the extracted data has been deleted.

DISH has also arranged for online monitoring and dark web scanning, and it has no evidence the data has been misused. The results of the monitoring are consistent with the confirmation that the data has been deleted. In particular, the monitoring has not revealed any indication that the personal information involved in this incident has been published, traded, sold, or otherwise misused.

DISH is also taking additional proactive measures to enhance its cyber defenses and overall security systems.

A copy of the individual notice is attached to this letter. If your office requires any further information in this matter, please contact me at (202) 471-3407 or lkalani@cozen.com.

Sincerely,

COZEN O'CONNOR

By: Lori Kalani

LK
Enclosures

<Return Name>
c/o Cyberscout
<Return Address>
<City> <State> <Zip>

<FirstName> <middle name> <LastName>
<Address1>
<Address2>
<City><State><Zip>

May x, 2023

Notice of Data Breach

<first name> <middle name> <last name>,

As you may know, DISH announced a cybersecurity incident in late February that affected our internal servers and IT telephony and involved the extraction of certain data from our IT systems.

We have since determined that the extracted data includes some of your personal information. We are not aware of any misuse of your information, and we have received confirmation that the extracted data has been deleted. Nevertheless, we are writing to notify you of this incident and to provide you with the information and resources contained in this letter, including the details of an offer for free credit monitoring through our vendor TransUnion.

What happened?

On February 23, 2023, we announced that we had experienced a network outage that affected internal servers and IT telephony. We immediately activated our incident response and business continuity plans designed to contain, assess and remediate the situation. We took steps to prevent further access to the impacted systems, including temporarily shutting down our internal network. The services of cyber-security experts and outside advisors were retained to assist in the evaluation of the situation, and once we determined that the outage was due to a cybersecurity incident, we promptly notified appropriate law enforcement authorities. In the following days, we further learned and disclosed that certain data had been extracted from our IT systems as part of this incident.

We have since determined that our customer databases were not accessed in this incident. However, we have confirmed that certain employee-related records and personal information (along with information of some former employees, family members and a limited number of other individuals) were among the data extracted.

The process of locating personal information in the extracted dataset and matching that information to individuals so that we could notify them was complex and time-consuming. This work was substantially completed on May 8, 2023. We then began notifying the list of persons whose personal information is confirmed to have been included, including you.

What information was involved?

The personal information that was in the extracted files appears to include your <<BREACHED ELEMENTS>>.

What are we doing?

1. **We are supporting those who personal information was extracted.** We have no evidence that any personal information was misused as a result of this incident. Nevertheless, certain states afford their residents a right to credit monitoring as a result of the incident. However, we have decided to offer credit monitoring to *everyone* whose personal information appears to have been extracted regardless of where they live. This offer of credit monitoring is provided for a period of two years at no cost to you through our vendor, TransUnion. Please see *Attachment A* for details regarding these credit monitoring services, as well as how to enroll using your unique code. **You must enroll by August 31, 2023 to receive these services.**

2. **We have received confirmation that the extracted data has been deleted.**

3. **We are conducting online monitoring and dark web scanning, and we have no evidence the extracted data has been misused.** The results of the monitoring are consistent with the confirmation that the extracted data has been deleted. In particular, the monitoring has not revealed any evidence that your personal information has been published, traded, sold, or otherwise misused.

4. **We are taking additional proactive measures with our systems and processes.** In addition to the above actions, DISH has taken steps to enhance its cyber defenses and overall security systems.

What can you do?

In addition to deciding whether to enroll in credit monitoring, we encourage you to consider the following.

- It is always a good idea to regularly review your account statements and credit history for any signs of unauthorized transactions or activity, and to remain vigilant against threats of identity theft or fraud; and

- If you ever suspect you are the victim of identity theft or fraud, you can contact your local police. Additional information about how to protect your identity is contained in *Attachment B*.

Would you like more information?

DISH has established a dedicated call center to answer questions about the cybersecurity incident as well as the services that we are offering to you. If you have any questions, please call 1-833-570-3074 Monday through Friday from 6am – 6pm Mountain Time, excluding holidays. We sincerely regret any inconvenience that this incident may have caused you. Our team has worked hard to quickly fix and limit any impacts the incident could have on you, and we appreciate your patience.

Sincerely,

The DISH Security Team

Attachment A (Details of the Offer of Credit Monitoring)

Attachment B (Additional Information)

Attachment A – Information About Credit Monitoring Offer

In response to the cybersecurity incident, we are offering you access to two years of **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services provide you with alerts for two years from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

How do I enroll in the free services?

To enroll in Credit Monitoring services at no charge, please log on to **https://secure.identityforce.com/benefit/dishcorp** and follow the instructions provided. When prompted please provide the following unique code to receive services: **<unique code>.**

In order for you to receive the services described above, you must enroll by August 31, 2023. The enrollment requires an internet connection and e-mail account and may not be available to minors under 18 years of age. Please note that when signing up for services, you may be asked to verify personal information for your own protection to confirm your identity.

Representatives are available to assist you with questions regarding this incident between the hours of 6:00 a.m. and 6:00 p.m. Mountain Time, Monday through Friday, excluding holidays. Please call the help line 1-833-570-3074 and supply the fraud specialist with your unique code listed above.

Attachment B – Information for U.S. Residents

ADDITIONAL INFORMATION

To protect against possible fraud, identity theft or other financial loss, you should always remain vigilant, to review your account statements and to monitor your credit reports. Provided below are the names and contact information for the three major U.S. credit bureaus and additional information about steps you can take to obtain a free credit report and place a fraud alert or security freeze on your credit report. If you believe you are a victim of fraud or identity theft you can contact your local law enforcement agency, your state's attorney general, or the Federal Trade Commission. Please know that contacting us will not expedite any remediation of suspicious activity.

INFORMATION ON OBTAINING A FREE CREDIT REPORT

U.S. residents are entitled under U.S. law to one free credit report annually from each of the three major credit bureaus. To order your free credit reports, visit www.annualcreditreport.com or call toll-free at +1 (877) 726-1014.

INFORMATION ON IMPLEMENTING A FRAUD ALERT OR SECURITY FREEZE

You may contact the three major credit bureaus at the addresses below to place a fraud alert on your credit report. A fraud alert indicates to anyone requesting your credit file that you suspect you are a possible victim of fraud. A fraud alert does not affect your ability to get a loan or credit. Instead, it alerts a business that your personal information might have been compromised and requires that business to verify your identity before issuing you credit. Although this may cause some short delay if you are the one applying for the credit, it might protect against someone else obtaining credit in your name.

A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing or other services.

A credit reporting agency may not charge you to place, temporarily lift, or permanently remove a security freeze.

To place a fraud alert or security freeze on your credit report, you must contact the three credit bureaus below:

Equifax: Consumer Fraud Division P.O. Box 740256 Atlanta, GA 30374 +1 (888) 766-0008 www.equifax.com	Experian: Credit Fraud Center P.O. Box 9554 Allen, TX 75013 +1 (888) 397-3742 www.experian.com	TransUnion: TransUnion LLC P.O. Box 2000 Chester, PA 19022-2000 +1 (800) 680-7289 www.transunion.com

To request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, the addresses where you have lived over those prior five years;
5. Proof of current address such as a current utility bill or telephone bill; and
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.).

You may also contact the U.S. Federal Trade Commission ("FTC") for further information on fraud alerts, security freezes, and how to protect yourself from identity theft. The FTC can be contacted at 400 7th St. SW, Washington, DC 20024; telephone +1 (877) 382-4357; or www.consumer.gov/idtheft.

ADDITIONAL RESOURCES

Your state attorney general may also have advice on preventing identity theft, and you should report instances of known or suspected identity theft to law enforcement, your state attorney general, or the FTC.

California Residents: Visit the California Office of Privacy Protection (https://oag.ca.gov/privacy) for additional information on protection against identity theft.

Connecticut Residents: The Attorney General can be contacted by emailing attorney.general@ct.gov or visiting portal.ct.gov/AG.

District of Columbia Residents: The District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; oag@dc.gov, and www.oag.dc.gov.

Iowa Residents: The Attorney General can be contacted at Office of Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, Iowa 50319, +1 (515) 281-5164, www.iowaattorneygeneral.gov. You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

Kentucky Residents: The Attorney General can be contacted at Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: +1 (502) 696-5300.

Maryland Residents: The Attorney General can be contacted at Office of Attorney General, 200 St. Paul Place, Baltimore, Maryland 21202; +1 (888) 743-0023; or www.marylandattorneygeneral.gov.

Massachusetts Residents: You may contact the Office of the Massachusetts Attorney General, 1 Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html. You have the right to obtain a police report if you are a victim of identity theft.

New Mexico Residents: You have rights under the federal Fair Credit Reporting Act (FCRA), which governs the collection and use of information pertaining to you by consumer reporting agencies. For more information about your rights under the FCRA, please visit www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

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

North Carolina Residents: The Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; +1 (919) 716-6400; or www.ncdoj.gov.

Oregon Residents: The Attorney General can be contacted at Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, +1 (877) 877-9332 (toll-free in Oregon), +1 (503) 378-4400, or www.doj.state.or.us. You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

Rhode Island Residents: The Attorney General can be contacted at 150 South Main Street, Providence, Rhode Island 02903; +1 (401) 274-4400; or www.riag.ri.gov. You may also file a police report by contacting local or state law enforcement agencies.