

Appendix

Between December 24, 2024 and December 27, 2024, an unauthorized actor viewed and obtained files stored on systems at a small number of iHeartMedia + Entertainment, Inc.'s ("iHeart") local stations. As soon as iHeart became aware, it immediately implemented its response protocols, took measures to contain the activity, and launched an investigation. Additionally, a cybersecurity firm that has assisted other companies in similar situations was engaged, and iHeart notified law enforcement.

iHeart conducted a careful review of the files and, on April 11, 2025, determined that one or more of the files contained the names and one or more of the following for 11 Nebraska residents: Social Security numbers, tax identification numbers, driver's license numbers, state identification card numbers, passport numbers, financial account numbers, and/or payment card numbers.

Today, April 30, 2025, iHeart is mailing notification letters via United States Postal Service First-Class mail to the Nebraska residents. A sample copy of the notification letter is enclosed. iHeart is offering one year of complimentary credit monitoring and identity protection services to the residents whose Social Security numbers, tax identification numbers, driver's license numbers, or state identification card numbers were involved. iHeart also has established a dedicated, toll-free call center that the residents can call to obtain more information regarding the incident.

To help prevent something like this from happening again, iHeart has strengthened its existing security measures.



Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

Postal Endorsement Line

<<Full Name>>

<<Address 1>>

<<Address 2>>

<<Address 3>>

<<City>>, <<State>> <<Zip>>

<<Country>>

***Postal IMB Barcode

<<Date>>

Notice of Data Breach

Dear <<Full Name>>:

Because iHeartMedia + Entertainment, Inc. recognizes the importance of protecting information, we are writing to let you know that we have identified and addressed a security incident involving some of your information. This notice explains the incident, the measures we have taken in response, and some additional steps you may consider taking.

What Happened? Between December 24, 2024, and December 27, 2024, an unauthorized actor viewed and obtained files stored on systems at a small number of our local stations. As soon as we became aware, we immediately implemented our response protocols, took measures to contain the activity, and launched an investigation. Additionally, a cybersecurity firm that has assisted other companies in similar situations was engaged, and we notified law enforcement.

We conducted a careful review of the files and, on April 11, 2025, determined that one or more of the files contained your information.

What Information Was Involved? The information included your name, passport number or other governmental identification number, date of birth, financial account information, payment card information, health information, and/or health insurance information.

What We Are Doing. We wanted to make you aware of this incident and to assure you that we take it seriously. We regret that this incident occurred and apologize for any inconvenience it may cause, and to prevent similar occurrences in the future we have strengthened our existing security measures.

What You Can Do. We encourage you to remain vigilant by reviewing your financial account statements and credit reports for any unauthorized activity. If you see charges or activity that you did not authorize, please contact the relevant financial institution or credit bureau immediately. For more information on some additional steps you can take, please review the pages that follow this letter.

For More Information. If you have any questions, please call 855-260-0508, Monday through Friday, between 9:00 a.m. and 9:00 p.m. Eastern Time (excluding holidays).

Sincerely,

iHeartMedia + Entertainment, Inc.

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity over the next 12 to 24 months. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-888-378-4329
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 1000, Chester, PA 19016, www.transunion.com, 1-833-799-5355

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

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

Fraud Alerts and Security Freezes

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active-Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- *Equifax Security Freeze*, PO Box 105788, Atlanta, GA 30348, www.equifax.com
- *Experian Security Freeze*, PO Box 9554, Allen, TX 75013, www.experian.com
- *TransUnion Security Freeze*, PO Box 160, Woodlyn, PA 19094, www.transunion.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

Protecting Health Insurance or Medical Information: It is always advisable to review any statements you may receive from your health insurer or healthcare providers. If you see charges for services that you did not receive, contact your insurer or provider immediately.

iHeartMedia + Entertainment, Inc. is located at 125 West 55th Street 12th Floor, New York, NY 10019 and can be reached at (210) 822-2828.

Additional Information for Residents of the Following States:

Maryland: You may contact and obtain information from your state attorney general at: *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.marylandattorneygeneral.gov/

New York: You may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection*, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, <http://www.dos.ny.gov/consumerprotection>; and *New York State Office of the Attorney General*, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov>

North Carolina: You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov

Rhode Island: This incident involves 1 individual in Rhode Island. Under Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: *Rhode Island Attorney General's Office*, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov

New Mexico: A Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street NW, Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies 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 reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.