
From: Radio.com Customer Support Team <datasecurityincident@entercom.com>
Sent: Friday, March 6, 2020 3:13 PM
To: Travers.Bray@experian.com
Subject: [TEST] Notice of Data Breach



Notice of Data Breach

Dear Radio.com User:

Entercom Communications Corp. (“Entercom”), which owns and operates Radio.com, is writing to inform you of an incident that may affect the security of your Radio.com username and password. We take this incident very seriously and are providing you with information and access to resources so that you can better protect against the possibility of misuse of this information, should you feel it appropriate to do so.

What Happened?

In September 2019, Entercom experienced a cyber-attack. We immediately began an investigation with assistance from outside data privacy and computer forensics specialists to determine the nature and scope of the incident. As part of our investigation into that attack, we became aware of unauthorized activity relating to third-party cloud hosting services, which we use to store information relating to Radio.com users.

Specifically, our investigation determined that for approximately three (3) hours on August 4, 2019, an unauthorized actor accessed information relating to Radio.com users contained in database backup files. After a thorough and intensive review process, the investigation recently confirmed the population of impacted individuals whose protected personal information was accessed by the unauthorized actor.

What Information Was Involved?

Our investigation determined the unauthorized actor gained access to the following types of information: name and Radio.com username and password.

What We Are Doing.

The confidentiality, privacy, and security of your personal information are among our highest priorities. We have taken and continue to take steps to prevent this type of incident from happening in the future, including by implementing password rotations, enabling multifactor authentication and stronger password policies for all cloud services, enhancing and broadening auditing based on best practices advised by third party experts, configuring alerts for certain behaviors using the relevant platforms, and providing additional training to staff on data security. We are also notifying regulatory authorities, as required.

What You Can Do.

You can review the attached Steps You Can Take to Protect Against Identity Theft and Fraud. We also strongly suggest that you change your password, as well as any account for which you used the same password. You may do so by: (a) signing out of the app and selecting “Forgot My Password” when next signing in; or (b) using the following Forgot Password link:

<https://myplayer.radio.com/mycbslocal/Pages/ForgotPassword.aspx>

For More Information.

We recognize that you may have questions not addressed in this letter. If you have additional questions, please call our toll-free dedicated assistance line at (855) 359-3626. This toll-free line is available Monday through Friday from 9:00 am to 11:00 pm Eastern and Saturday through Sunday from 11:00 am to 8:00 pm Eastern, excluding major US holidays.

We sincerely regret any inconvenience this incident may cause you. We remain committed to safeguarding the information in our care and will continue to take steps to ensure the security of our systems.

Sincerely,

Radio.com Customer Support Team

Steps You Can Take to Protect Your Information

Monitor Your Accounts/Credit Reports

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

You have the 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. The security 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 security 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 security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian

P.O. Box 9554
Allen, TX 75013
1-888-397-3742

www.experian.com/freeze/center.html

TransUnion

P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872

www.transunion.com/credit-freeze

Equifax

P.O. Box 105788
Atlanta, GA 30348-5788
1-800-685-1111

www.equifax.com/personal/credit-report-services

In order 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, provide the addresses where you have lived over the prior 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, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your 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 agencies listed below:

Experian

P.O. Box 9554
Allen, TX 75013
1-888-397-3742

www.experian.com/fraud/center.html

TransUnion

P.O. Box 160
Woodlyn, PA 19094
1-800-680-7289

www.transunion.com/fraud-victim-resource/place-fraud-alert

Equifax

P.O. Box 105788
Atlanta, GA 30348-5788
1-888-766-0008

www.equifax.com/personal/credit-report-services

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); 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.



March 9, 2020

Re: Notice of Data Breach

Dear _____ :

Entercom Communications Corp. (“Entercom”), which operates radio stations in the United States, including WPHT-AM, is writing to inform you of an incident that may affect the security of your personal information. We take this incident very seriously and are providing you with information and access to resources so that you can better protect against the possibility of misuse of this information, should you feel it appropriate to do so.

What Happened? In September 2019, Entercom experienced a cyber-attack. We immediately began an investigation with assistance from outside data privacy and computer forensics specialists to determine the nature and scope of the incident. As part of our investigation into that attack, we became aware of unauthorized activity relating to third-party cloud hosting services, which we use to store information relating to listeners who provide information to us.

Specifically, our investigation determined that for approximately three (3) hours on August 4, 2019, an unauthorized actor accessed information relating to our listeners who submit information to us in database backup files. After a thorough and intensive review process, the investigation recently confirmed the population of impacted individuals whose protected personal information was accessed by the unauthorized actor.

What Information Was Involved? Our investigation determined that the impacted database backup files contained, and the unauthorized actor may have accessed, the following types of your personal information: name, Social Security number, and driver’s license number.

What We Are Doing. The confidentiality, privacy, and security of your personal information are among our highest priorities. We have taken and continue to take steps to prevent this type of incident from happening in the future, including by implementing password rotations, enabling multifactor authentication and stronger password policies for all cloud services, enhancing and broadening auditing based on best practices advised by third party experts, configuring alerts for certain behaviors using the relevant platforms, and providing additional training to staff on data security. We are also notifying regulatory authorities, as required.

As an additional precaution, Entercom is offering you access to twelve (12) months of complimentary credit monitoring and identity theft restoration services through ID Experts at no cost to you. Details of this offer and instructions on how to enroll in these services are enclosed with this letter.

What You Can Do. You can enroll in the complimentary credit monitoring services being offered to you. Please also review the attached *Steps You Can Take to Protect Against Identity Theft and Fraud*.

For more information. We recognize that you may have questions not addressed in this letter. If you have additional questions, please call our toll-free dedicated assistance line at (866) 977-0894. This toll-free line is available Monday through Friday from 9:00 am to 9:00 pm Eastern Standard Time, excluding major US holidays.

We sincerely regret any inconvenience this incident may cause you. We remain committed to safeguarding the information in our care and will continue to take steps to ensure the security of our systems.

Sincerely,

Entercom Customer Support Team

Steps You Can Take to Protect Your Information

Enroll in Credit Monitoring

As an added precaution, and at no cost to you, we arranged to have ID Experts provide identity monitoring for 12 months. ID Experts is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Dark Web Monitoring, and Identity Recovery Assistance. It is incumbent upon you to enroll in these services, as we are not able to act on your behalf to enroll you in the credit monitoring service. To enroll and start monitoring your personal information, please follow the steps below:

- Visit <https://app.myidcare.com/account-creation/protect> to enroll in and take advantage of your identity monitoring services.
- You have until **October 1, 2020** to enroll in your identity monitoring services.
- Membership Number:
- If you have questions about enrolling in these services, please call **1-800-939-4170**

ADDITIONAL DETAILS REGARDING YOUR TWELVE MONTH ID EXPERTS MONITORING SERVICES

MyIDCare will include one-year enrollment(s) into the following services:

SINGLE BUREAU CREDIT MONITORING - Monitoring of credit bureau for changes to the member's credit file such as new credit inquires, new accounts opened, delinquent payments, improvements in the member's credit report, bankruptcies, court judgments and tax liens, new addresses, new employers, and other activities that affect the member's credit record.

CYBERSCANTM - Dark Web monitoring of underground websites, chat rooms, and malware, 24/7, to identify trading or selling of personal information like SSNs, bank accounts, email addresses, medical ID numbers, driver's license numbers, passport numbers, credit and debit cards, phone numbers, and other unique identifiers.

IDENTITY THEFT INSURANCE - Identity theft insurance will reimburse members for expenses associated with restoring their identity should they become a victim of identity theft. If a member's identity is compromised, the policy provides coverage for up to \$1,000,000, with no deductible, from an A.M. Best "A-rated" carrier. Coverage is subject to the terms, limits, and/or exclusions of the policy.

FULLY-MANAGED IDENTITY RECOVERY - ID Experts' fully-managed recovery service provides restoration for identity theft issues such as (but not limited to): account creation, criminal identity theft, medical identity theft, account takeover, rental application, tax fraud, benefits fraud, and utility creation. This service includes a complete triage process for affected individuals who report suspicious activity, a personally assigned IDCare Specialist to fully manage restoration of each case, and expert guidance for those with questions about identity theft and protective measures.

Monitor Your Accounts/Credit Reports

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

You have the 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. The security 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 security 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 security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian

P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion

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

Equifax

P.O. Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
www.equifax.com/personal/credit-report-services

In order 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, provide the addresses where you have lived over the prior 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, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended “fraud alert” on your 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 agencies listed below:

Experian

P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/fraud/center.html

TransUnion

P.O. Box 2000
Chester, PA 19016
1-800-680-7289
www.transunion.com/fraud-victim-resource/place-fraud-alert

Equifax

P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008
www.equifax.com/personal/credit-report-services

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); 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.