

SAMPLE NOTICE TO CONSUMERS

September 2, 2015

First Name, Last Name
Address line
Address line 2
City, State, Zip Code

Dear

ReverbNation is contacting you about an incident regarding a possible breach of your personal information. We are committed to protecting your privacy, so please review the following important information.

ReverbNation was recently contacted by law enforcement and alerted that an individual had illegally sought to gain unauthorized access to some of our customer's user data. In January 2014, an individual, who has since been identified and charged, illegally accessed a ReverbNation vendor's computer systems and ultimately gained unauthorized access to user information contained in a backup of our database. We believe that the date range of the unauthorized access was, at most, January through May 2014. We have since taken additional steps to further secure our system against security breaches. The information included in the database may have included your name, social security number, employer identification number, e-mail address, encrypted password, postal address, phone number, date of birth, and possibly other user information you may have provided to us.

No credit card data of any kind was accessed, as we never retain your credit or debit card information in our database.

We take the confidentiality of our customer information very seriously, so we are providing you with specific information below to help protect your personal and/or financial records. Out of an abundance of caution, in order to protect the privacy of all of our users, we are strongly encouraging all users to change their ReverbNation passwords.

Change Your Password. Although your password was encrypted it is possible for a person with enough computing power to guess an encrypted password by testing particularly weak or obvious passwords. You should also change your password on any other accounts or websites which share your previous ReverbNation password. Additionally, you should avoid using identical passwords on multiple websites. For additional help with password security, we also recommend password management tools like 1Password and LastPass.

Place a fraud alert on your credit report. We recommend that you place a fraud alert on your credit report. A fraud alert is free of charge and easy to place. You may contact toll-free any one of the three major credit bureaus listed below. As soon as one bureau confirms your report, the others are simultaneously notified on your behalf.

Equifax
P.O. Box 740256
Atlanta, GA 30374
888-766-0008

Experian
475 Anton Blvd
Costa Mesa, CA 92626
888-397-3742

TransUnion LLC
P.O. Box 2000
Chester, PA 19022-2000
800-680-7289

Obtain a copy of your free credit report. You may also obtain a free copy of your credit report from each of the three major credit reporting bureaus once every 12 months by visiting www.annualcreditreport.com, calling toll-free (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, Georgia 30348. It is recommended that you continue

to monitor your free credit reports for incidents of fraud and identity theft. You may purchase a copy of your credit report by contacting one of the three major credit reporting bureaus above.

Monitor your credit reports and account statements. Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you remain vigilant by monitoring your credit reports and account statements periodically. Doing so can help you spot problems and address them quickly.

Notify law enforcement of any suspicious activity. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to the appropriate law enforcement authorities, your state attorney general, and/or the FTC.

Additional resources to protect against identity theft. You can find additional information to help protect yourself from identity theft, including information about fraud alerts and security freezes, by contacting one of the three major credit bureaus listed above, or by visiting the FTC's website at www.ftc.gov/idtheft, by calling 1-877-ID-THEFT (1-877-438-4338), or by writing to the Federal Trade Commission, 600 Pennsylvania Ave., NW, Washington, DC 20580.

- **Maryland residents** may wish to review information provided by the Maryland Attorney General on how to avoid identity theft at <http://www.oag.state.md.us/idtheft>, or by sending an e-mail to idtheft@oag.state.md.us, by calling (888) 743-0023, or by writing to the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, 16th Floor, Baltimore, MD 21202.
- **North Carolina residents** may wish to review information provided by the North Carolina Attorney General at <http://www.ncdoj.gov>, by calling (877) 566-7226, or by writing to the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699.
- **Wisconsin residents** may submit a written request to ReverbNation to learn the personal information that may have been acquired.

How to contact us. If you have any questions or if you would like additional information regarding this cyberattack you may contact us at (877) 202-8667, Monday through Friday, 8:30 am – 5:00 pm EST, e-mail us at privacy@reverbnation.com, or write us at P.O. Box 2086, Durham, NC 27702.

We apologize for the inconvenience. We thank you for being part of the ReverbNation community, and we appreciate the continued opportunity to serve you.

Respectfully,

Michael Doernberg
Chief Executive Officer
ReverbNation