[DATE]

[Name]
[Street Address]
[City], [State] [ZIP]

Dear [Name],

TuneCore recently discovered suspicious activity on its servers, including the illegal collection of certain personal and account information. This information may have included your Social Security or taxpayer ID number and date of birth, as well as your royalty statements for the third quarter of 2015, showing the number of sales or downloads on different platforms, along with the contractual rate for them, and the sum of transactions. It may also have included your name, address, email address, TuneCore account number, and protected TuneCore password. In addition, if you provided us with billing information, the information illegally accessed may have included your billing address; the last 4 digits of your credit card number, as well as its expiration date; your bank name and the last 4 digits of your bank account number and the last 4 digits of your bank routing number; and the name and address associated with the bank account. TuneCore does not store any full financial account information.

Based on our investigation, it appears that there were suspicious log-ins to three of our servers in early November, and that on November 17th an unauthorized intruder illegally exported the information stored on them. Upon discovery that your information may have been illegally accessed, TuneCore promptly took action to protect you, and we are sending this notice to you without delay. Although we do not know the identity of the individual or individuals responsible for this attack, we are actively working with law enforcement to investigate the unlawful access to our servers, and we have retained a leading cybersecurity firm to help review our security protocols and provide guidance on additional steps we can take to prevent this from happening again.

TuneCore already had several important security measures in place, including manual review of all requests for payment, restricting access to our main website production servers, and protecting account passwords. Now, we have secured all of our environments with updated access controls and instituted more detailed network logging. We have assessed the vulnerability of other systems and we have not found any similar vulnerabilities or breach attempts. We have instituted a policy of access segregation among our environments so that the reuse of access keys is no longer allowed. We have also upgraded all encryption algorithms. All development and IT processes are under review for further security remediation and enhancement.

Finally, although TuneCore passwords are stored in a protected form, it is possible for a determined hacker with sufficient time, using advanced computing tools, to recover those passwords. Therefore, in an abundance of caution, on December 4 we sent you an email informing you that we invalidated your then-current TuneCore password, and requested that you log in to TuneCore as soon as possible to set a new password. If you have not already done so,

please log in to change your TuneCore password now. You should also change your password on any other accounts or websites that share your previous TuneCore password.

Your privacy and the security of your information are very important to us. To help safeguard you from misuse of your personal information, if you provided your Social Security number or taxpayer ID number to TuneCore, we have arranged monitoring of activity within the United States for twelve (12) months at no cost to you. **Information on how to enroll in this free service is provided on a separate page.** This service will provide you with extra security, but we encourage you to remain vigilant against fraud and identity theft by reviewing account statements and monitoring free credit reports for signs of fraud or identity theft. You can also get information about protecting yourself from identity theft, including how to place a security freeze on your credit, from the major credit reporting agencies, your state attorney general, and the Federal Trade Commission (FTC). The toll-free telephone numbers and addresses for the credit reporting agencies and FTC are included below.

Contact Information For Major Credit Reporting Agencies and FTC	
Equifax	(800) 525-6285; P.O. Box 105069, Atlanta, GA 30348; www.equifax.com
Experian	(888) 397-3742; P.O. Box 72, Allen, TX, 75013; www.experian.com
TransUnion	(800) 680-7289; P.O. Box 6790, Fullerton, CA 92834; www.transunion.com
FTC	1-877-ID-THEFT (1-877-438-4338); 600 Pennsylvania Ave., NW, Washington, DC 20580; www.ftc.gov/idtheft

- **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.

You also may want to put a security freeze on your credit file, and can do so by providing identification information to the credit reporting agencies, either online, through the mail, or by phone. A security freeze 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. However, using a security freeze may interfere with or delay your ability to obtain credit. In order for the freeze to be fully effective, you must place a separate freeze on your credit file with each credit reporting agency. Additionally, if you request a security freeze from a consumer reporting agency there may be a fee of up to $10 to place, lift, or remove the security freeze.

Finally, although TuneCore does not keep full financial information, as a precautionary measure, you should monitor activity on your card and account statements for the next 12 to 24 months and promptly report incidents of suspected identity theft to your financial institution or card

provider. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to the proper law enforcement authorities, your state attorney general, and/or the FTC.

TuneCore takes data security very seriously, especially the security of our customers' personal and account information. We know this security breach may have had an impact on you, causing you frustration and concern, but we are working to make things right for you. If you have any further questions, please contact us via e-mail at info@tunecore.com. You may also always visit the website, www.tunecore.com, and you can also call toll-free **866-329-9387.**

Sincerely,

Scott Ackerman
CEO, TuneCore

How to Enroll In Free Identity Monitoring

You can enroll in a professional identity monitoring service (First Watch ID) provided by First Watch Technologies, Inc. You can sign up for this service anytime between now and January 22, 2016 using the verification code listed below. To enroll in this service, simply call **866-329-9387** Monday through Friday between the hours of 9 a.m. and 7 p.m. EST or go to www.firstwatchid.com and:

* Click on the Verification Code button.
* Enter the appropriate information, including your unique 12-digit verification code: _____.

After enrollment, you will receive one year of proactive identity monitoring. First Watch ID will monitor thousands of databases and billions of records on your behalf to look for suspicious activity that could indicate the beginning steps of identity theft. If suspicious activity is found, First Watch will place a personal phone call to you (at the telephone number that you provide) to determine if the suspicious activity is potentially fraudulent.

Additionally, if you enroll, First Watch provides you with easy online access to monitor your credit activity using the three major credit bureau services. Each credit bureau will provide you one free credit report annually. First Watch suggests you request your free credit report from one bureau at a time every four months. This allows you to monitor credit activity three times per year. First Watch will send you an email (at the email address you provide) every four months reminding you to request your free credit report from the appropriate bureau.

The First Watch ID service also includes up to $1,000,000.00 of identity theft insurance with $0 deductible, along with identity restoration coverage (certain limitations and exclusions may apply).