

[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 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 some 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 that 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, though 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. 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.

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

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](mailto:info@tunecore.com). You may also always visit the website, [www.tunecore.com](http://www.tunecore.com).

Sincerely,

Scott Ackerman  
CEO, TuneCore