TM Acquisition, LLC
2460 N. First Street, Suite 260
San Jose, CA 95131

January 13, 2012

VIA EXPRESS MAIL

New Hampshire Department of Justice
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notice of Security Breach

Dear Sir or Madam:

Pursuant to N.H. Rev. Stat. § 359-C:20, TM Acquisition, LLC, doing business as Trymedia, and a subsidiary of RealNetworks, Inc., provides you with this notice concerning a data security breach.

We recently became aware of a criminal intrusion into our ActiveStore Web-based storefront application that processes purchases of digital games made by customers on our partners' Web sites. We believe the intruders may have been able to intercept and obtain cardholder names, credit card account numbers, expiration dates, security codes, postal addresses, email addresses, and passwords to optional user accounts on ActiveStore storefronts from a portion of transactions flowing through the ActiveStore application between November 4, 2011, and December 2, 2011.

Immediately upon learning of the intrusion, we took the affected systems offline and took steps to address the vulnerability that led to this incident. We engaged external experts to investigate the incident and have taken additional steps to enhance our information security controls. We have notified law enforcement authorities and are cooperating with their efforts to identify those responsible for the intrusion. We also have notified all major credit card brands of the incident.

We plan to notify approximately 12,456 of our users, including approximately 96 New Hampshire residents, of this potential breach in the security of their personal information. A copy of the notice to be distributed to New Hampshire residents is enclosed. We are offering affected consumers in all U.S. states a free twelve-month subscription to a credit monitoring and identity theft protection product. We plan to distribute notices to all affected users for whom we have ascertained verified postal addresses (who comprise more than 95% of affected users) on or around January 17, 2012. We are working to obtain verified postal addresses for the remainder of affected users, which may include some New Hampshire residents, and plan to notify them expeditiously.

Sincerely,
TM Acquisition, LLC d/b/a Trymedia

Enclosure

Experian Consumer Direct
PO Box 483
Chanhassen, MN 55317

January __, 2012

[Name]
[Address 1 & 2]
[City/State/Zip]

Re: Notice of Security Incident

Dear [Name]:

We are contacting you because you purchased or began to purchase a digital game between November 4, 2011 and December 2, 2011. Your credit card information was processed through our Trymedia ActiveStore, which manages many digital game storefronts on behalf of retailers.

An illegal and unauthorized intrusion regrettably occurred, which may have caused your personal information to be compromised. The intrusion has been stopped and we don't yet know that any fraudulent transactions have actually occurred. We do, however, want to make you aware of what has occurred and to provide you with information that you may use to protect your credit.

We deeply regret this event and we are working diligently to prevent any similar incidents from happening in the future.

Our highest and most immediate concern is the impact that this may have on you and in your confidence in us as a trusted merchant. We have enclosed a summary and a guide containing some recommended steps that you may take to help monitor and safeguard your identity and credit.

The following pages detail in depth what happened, recommendations on monitoring your identity and credit, fraud alerts, free credit reports, and our offer of a free complimentary one-year membership for ProtectMyID, a service that provides credit monitoring and identity theft resolution services. We have also listed a telephone number to reach out to for more information, and have established a website with additional information about the incident.

For Further Information. We hope you find the information in this letter useful. If you have any questions, please do not hesitate to contact our information hotline as follows:

Toll-Free Phone Number: 866-579-2216

You also may access additional information about this incident, including frequently asked questions, at a Web site we have established at www.trymedia.com/2011securityincident.

We sincerely apologize for any inconvenience this illegal intrusion may cause you. Please do reach out if you have any questions at all about this very unfortunate event.

Sincerely,

TM Acquisition, LLC (doing business as Trymedia)

WHAT HAPPENED

We recently became aware of a criminal intrusion into our ActiveStore Web-based storefront application that processes purchases of digital games made by customers on our partners' Web sites. We believe the intruders may have been able to intercept and obtain cardholder names, credit card account numbers, expiration dates, security codes, postal addresses, email addresses, and passwords to optional user accounts on ActiveStore storefronts from a portion of transactions flowing through the ActiveStore application between November 4, 2011, and December 2, 2011.

We are notifying you because you made, or attempted to make, a purchase of a digital game from a company that used the ActiveStore Web-based storefront application to process transactions on its Web site during the time period described above. Consequently, we believe that your personal information may have been exposed to the intruders.

Please know that safeguarding your personal information is very important to us. As described below, we have taken measures to address the intrusion and to offer a credit protection service to affected customers at no charge.

We believe that the intrusion has been contained. Immediately upon learning of the intrusion, we took the affected systems offline and took steps to address the vulnerability that led to this incident. We engaged external experts to investigate the incident and we have taken additional steps to enhance our information security controls. We notified all major credit card brands of the incident. We also have notified law enforcement authorities and are cooperating with their efforts to identify those responsible for the intrusion. This notice was not delayed as a result of a law enforcement investigation.

RECOMMENDED NEXT STEPS

We are notifying you of this incident so that you may take any additional steps you feel appropriate to reduce or eliminate harm. Below are precautionary steps that you may wish to consider, along with resources from which you may obtain additional information.

ActiveStore Accounts. If you set up an account on an ActiveStore storefront when you made a digital game purchase, you can change your password by going to the ActiveStore storefront(s) on which you purchased a digital game between November 4, 2011 and December 2, 2011 and follow the instructions on the storefront to change your password.

Prevention of Fraud and ID Theft. We encourage you to remain vigilant for incidents of fraud, identity theft, and other misuse of your personal information. In addition to taking other steps described in this letter, you should review your credit card statements and other account information carefully and immediately notify your card issuer in writing if you suspect fraudulent use. You may also wish to contact your card issuer to monitor for suspicious activity or to take other steps to protect your account, such as requesting that your card issuer close the account and reissue a new card with a different number.

Also, in addition to other recommended steps described in this letter, we encourage you to report suspected incidents of identity theft to local law enforcement, your state's Attorney General, or the Federal Trade Commission. Contact information for the Federal Trade Commission is given below.

Fraud Alerts. To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert places a statement on your credit report that directs a creditor to contact you before extending credit. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your record. An initial fraud alert lasts 90 days. To place an extended fraud alert, you will need to provide a copy of a police report and proof of your identity. Details are available on the credit-reporting agency Web sites listed below, or by calling the credit reporting agencies at the numbers listed below:

Equifax	Experian	TransUnion
P.O. Box 105069 Atlanta, GA 30348-5069	P.O. Box 1017 Allen, TX 75013	P.O. Box 6790 Fullerton, CA 92834-6790
800-525-6285	888-397-3742	800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

Free Credit Reports. Under U.S. law, you are entitled to one free credit report annually from each of the three national credit bureaus listed above. To order your free credit report, visit www.annualcreditreport.com, call toll-free at 877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission Web site at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three national credit bureaus provide free annual credit reports only through these methods.

We encourage you to obtain free annual credit reports and to review them for suspicious activity and inaccuracies. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing.

Contacting the FTC. In addition to your state Attorney General, you can contact the Federal Trade Commission to learn more about how to protect yourself from identity theft:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
877-IDTHEFT | 877-438-4338
www.ftc.gov
www.ftc.gov/bcp/edu/microsites/idtheft/consumers/index.html

ProtectMyID™. We are offering a complimentary one-year membership to Experian's ProtectMyID™ product. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft.

You may activate ProtectMyID by taking the following steps:

1. Ensure that you enroll by: April 30, 2012.
2. Visit the ProtectMyID Web Site: www.protectmyid.com/redeem or call 866-579-2216 to enroll.
3. Provide your activation code: [Experian-supplied code]

Once your ProtectMyID membership is activated, your credit report will be monitored daily for fifty leading indicators of identity theft. You'll receive timely credit alerts from ProtectMyID on any key changes in your credit report which could include new inquiries, new credit accounts, medical collections and changes to public records. Your complimentary 12-month ProtectMyID membership includes the following:

- **Credit Report**: A free copy of your Experian credit report.
- **Daily Credit Monitoring**: Alerts you of suspicious activity including new inquiries, newly opened accounts, delinquencies, or medical collections found on your Experian credit report.
- **Identity Theft Resolution**: If you have been a victim of identity theft, you will be assigned a dedicated, U.S.-based Experian Identity Theft Resolution Agent who will walk you through the fraud resolution process, from start to finish.

We sincerely regret any inconvenience this intrusion may cause you.

Sincerely,

TM Acquisition, LLC (doing business as Trymedia)