21615 N 7TH AVE
PHOENIX, AZ 85027

[Insert name]
[Insert address]

Dear [Insert name],

On August 18, 2014, Yandy.com discovered an unauthorized, external cyber-attack affecting its website. Yandy.com took immediate steps to stop the attack and restore the integrity and security of its website. The unauthorized intrusion permitted access to customer's payment card data which was submitted during the checkout process. Specifically, the information which may have been obtained included names, addresses, credit card or debit card numbers, expiration dates, CVV numbers, and email addresses. You are receiving this notification because it appears you were a customer on Yandy.com during the brief times frames that the unauthorized intrusion occurred.

Upon discovering the unauthorized intrusion, a report was filed with the Internet Crime Complaint Center, which is co-sponsored by the Federal Bureau of Investigation ("FBI") and the National White Collar Crime Center. We are unable to confirm any improper use of your personal information in connection with this incident. Nonetheless, we are sending this advisory to you and other individuals whose personal information may have been accessed to make you aware of this incident so that you can take steps to protect yourself and minimize the possibility of misuse of your information. The attached sheet describes steps you can take to protect your identity, credit and personal information.

At Yandy, your trust is something we value above all else. Since discovering this issue we have worked diligently and expeditiously to ensure the safety of our customer information. We sincerely apologize for this situation and any inconvenience it may cause you.

We treat all sensitive customer information in a confidential manner and are proactive in the careful handling of such information. We continue to assess and modify our privacy and data security policies and procedures to prevent similar situations from occurring.

If you have questions or concerns you can contact us at 1-844-236-1015.

Sincerely,

Yandy.com Team

PLEASE TURN PAGE FOR ADDITIONAL INFORMATION

What You Should Do to Protect Your Personal Information

We recommend you remain vigilant and consider taking one or more of the following steps to protect your personal information:

1. Contacting the nationwide credit-reporting agencies as soon as possible to:
   - Add a fraud alert statement to your credit file at all three national credit-reporting agencies: Equifax, Experian, and TransUnion. You only need to contact one of the three agencies listed below; your request will be shared with the other two agencies. This fraud alert will remain on your credit file for 90 days.
   - Remove your name from mailing lists of pre-approved offers of credit for approximately six months.
   - Receive a free copy of your credit report by going to www.annualcreditreport.com.

Equifax	Experian	TransUnion
P.O. Box 740256	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19022
(800) 525-6285	(888) 397-3742	(800) 888-4213
www.equifax.com	www.experian.com/consumer	www.transunion.com

2. If you aren't already doing so, please pay close attention to all bills and credit-card charges you receive for items you did not contract for or purchase. Review all of your bank account statements frequently for checks, purchases or deductions not made by you. Note that even if you do not find suspicious activity initially, you should continue to check this information periodically since identity thieves sometimes hold on to stolen personal information before using it.

3. The Federal Trade Commission ("FTC") offers consumer assistance and educational materials relating to identity theft, privacy issues and how to avoid identity theft. The FTC can be contacted either by visiting www.ftc.gov, www.consumer.gov/idtheft, or by calling (877) 438-4338. If you suspect or know that you are the victim of identity theft, you should contact local police and you also can report this to the Fraud Department of the FTC, who will collect all information and make it available to law-enforcement agencies. Contact information for the FTC is:

   Federal Trade Commission
   Consumer Response Center
   600 Pennsylvania Avenue
   NW Washington, DC 20580

4. *For North Carolina Residents*: For more information on identity theft please contact either the Federal Trade Commission at the contact information provided above, or North Carolina's Attorney General's Office, Address: 9001 Mail Service Center, Raleigh, NC 27699-9001; Telephone: (919) 716-6400; Fax: (919) 716-6750; website: www.ncdoj.com/

5. *For Maryland Residents*: The contact information for the State's Office of the Attorney General, which provides information about how to avoid identity theft, is

   Honorable Douglas F. Gansler
   Office of the Attorney General
   200 St. Paul Place
   Baltimore, MD 21202

   Website: http://www.oag.state.md.us
   Telephone number: (888) 743-0023
   (toll-free in Maryland)

6. *For West Virginia Residents*: You have the right to obtain a copy of the applicable police report relating to this incident. You may want to place a "security freeze" on your credit account. This means that your credit account cannot be shared with potential creditors. A security freeze can help prevent new account identity theft. If you would like to request a security freeze be placed on your account, you must write by certified or overnight mail (see addresses at link below) to each of the three credit reporting agencies, or through the

electronic or Internet method made available by the credit reporting agencies. Credit reporting agencies charge a $5 fee to place or remove a security freeze, unless you provide proof that you are a victim of identity theft, in which case there is no fee. A copy of your police report or an investigative report or written FTC complaint documenting identity theft must be included to avoid a fee. In your request, you also must include (documentation for both the spouse and the victim must be submitted when requesting for the spouse's credit report) (i) a copy of either the police report or case number documenting the identity theft, if you are a victim of identity theft; (ii) your full name (including middle initial as well as Jr., Sr., II, III, etc.,) address, Social Security number, and date of birth; (iii) if you have moved in the past 5 years, the addresses where you have lived over the prior 5 years; (iv) proof of current address such as a current utility bill or phone bill; (v) a photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.); and, if applicable (vi) payment by check, money order or credit card (Visa, Master Card, American Express or Discover cards only.) For more information, go to http://www.consumersunion.org/pdf/security/securityWV.pdf

Alternatively, you could place a fraud alert with the credit reporting agencies. This will flag your file with a statement that says you may be a victim of fraud and that creditors should phone you before extending credit. To place a fraud alert on your credit file call the fraud department of one of the three credit reporting agencies -- Experian, Equifax, or TransUrban (see above). When you request a fraud alert from one agency, it will notify the other two for you. You can place an initial fraud alert for only 90 days, and you may cancel the fraud alerts at any time.