

April 25, 2014

VIA CERTIFIED MAIL RETURN RECEIPT REQUESTED

Office of the New Hampshire Attorney General
Consumer Protection & Antitrust Bureau
33 Capitol Street
Concord, NH 03301

Re: Legal Notice of Potential Information Security Incident

Dear Sirs or Madams,

I write to inform you of a potential security incident involving personal information maintained by Boomerang Tags that involved approximately 219 New Hampshire residents.

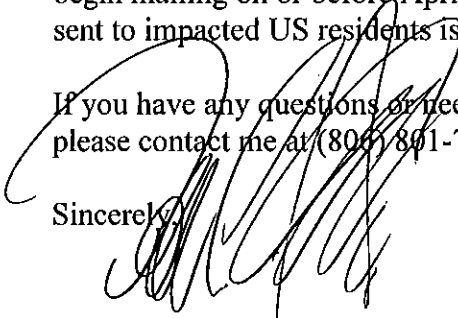
Recently, a service provider of Boomerang Tags discovered that unauthorized individuals or entities installed malicious software on the computer server we use to host our website, www.boomerangtags.com. ("Website"). We believe the malware compromised the payment card data of customers who made purchases through the Website between July 4, 2013 and February 18, 2014, including name, address, payment card account number, card expiration date and security code.

Keeping personal information secure is of the utmost importance to us, and we took steps to address and contain the incident the same day it was discovered. We promptly engaged a computer forensic investigator to perform an investigation, and we have already taken measures designed to prevent this from happening again the future, such as replacing our old payment card processor and designing an entirely new website with additional security features that will be launched in the near future.

Boomerang Tags is notifying affected individuals and these notifications will begin mailing on or before April 25, 2014. A copy of the form of notice being sent to impacted US residents is attached for your reference.

If you have any questions or need further information regarding this incident, please contact me at (800) 801-7334 or don@boomerangtags.com.

Sincerely,



Don Carrick
Owner, Boomerang Tags
Enclosure

Dear Customer:

We are writing to inform you of a security incident involving certain personal information you provided while shopping at BoomerangTags.com (the "Website"). As a precaution we are providing this notice and outlining some steps you may take to help protect yourself. We sincerely apologize for any inconvenience or concern this may cause you.

We recently learned that unauthorized individuals or entities installed malicious software on the computer server we use to host our Website. We believe the malware compromised the payment card data of visitors that made payment card purchases through the Website between July 4, 2013 and February 18, 2014, including name, address, payment card account number, card expiration date and security code. According to our records, you made a payment card purchase at the Website during that timeframe, and your information may be at risk.

We value our relationship with you and sincerely regret any inconvenience or concern this incident may cause. Keeping your personal information secure is of the utmost importance to us, and we took steps to address and contain the incident the same day it was discovered. We also promptly engaged a computer forensic investigator to perform an investigation, and we have already taken measures designed to prevent this from happening again the future, such as replacing our old payment processor and designing an entirely new website with additional security features that will be launched in the near future.

We want to make you aware of steps you can take to guard against identity theft or fraud. We recommend that you review your credit and debit card account statements as soon as possible in order to determine if there are any discrepancies or unusual activity listed. You should remain vigilant and continue to monitor your statements for unusual activity going forward. If you see anything you do not understand or that looks suspicious, or if you suspect that any fraudulent transactions have taken place, you should call the bank that issued the credit or debit card immediately.

We also recommend you carefully check your credit reports for accounts you did not open or for inquiries from creditors you did not initiate. If you see anything you do not understand, call the credit agency immediately. If you find any suspicious activity on your credit reports, call your local police or sheriff's office. Also, please review the enclosed "Information about Identity Theft Protection" reference guide that describes additional steps you may take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection, and details on how to place a fraud alert or a security freeze on your credit file.

If you have any questions or need further information regarding this incident, you may contact us by sending an email to: service@boomerangtags.com.

Again, we are sorry for any inconvenience or concern this event may have caused.

Sincerely,

Don Carrick
Owner
BoomerangTags.com

Information about Identity Theft Protection

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax
P.O. Box 740241
Atlanta, GA 30374-0241
800-685-1111
www.equifax.com

Experian
P.O. Box 9532
Allen, TX 75013
888-397-3742
www.experian.com

TransUnion
P.O. Box 6790
Fullerton, CA 92834-6790
800-916-8800
www.transunion.com

When you receive your credit reports, look them over carefully. Look for accounts you did not open. Look for inquiries from creditors that you did not initiate. And look for personal information, such as home address, that is not accurate. If you see anything you do not understand, call the credit agency at the telephone number on the report. If you do find suspicious activity on your credit reports, call your local police or sheriff's office and file a police report of identity theft. Get a copy of the police report. You may need to give copies of the police report to creditors to clear up your records.

You should remain vigilant with respect to reviewing your account statements and credit reports, and you should promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the Federal Trade Commission ("FTC").

You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding and protection against identity theft: Federal Trade Commission, Consumer Response Center 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

For residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General: Maryland Office of the Attorney General, Consumer Protection Division 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us

For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from North Carolina Attorney General's Office: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov

Fraud Alerts: There are also two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for

seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies at the addresses or toll-free numbers listed below:

Equifax
P.O. Box 740241
Atlanta, GA 30374-0241
877-478-7625
www.equifax.com

Experian
P.O. Box 9532
Allen, TX 75013
888-397-3742
www.experian.com

TransUnion
Fraud Victim Assistance
Division
P.O. Box 6790
Fullerton, CA 92834-6790
800-680-7289
www.transunion.com

Credit Freezes: You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally \$5 to \$20 per action at each credit reporting company. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information.

Equifax
P.O. Box 105788
Atlanta, GA 30348
www.equifax.com

Experian
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion
Fraud Victim Assistance
Division
P.O. Box 6790
Fullerton, CA 92834-6790
www.transunion.com

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed above.