DICKSTEINSHAPIROLLP

1825 Eye Street NW | Washington, DC 20006-5403
TEL (202) 420-2200 | FAX (202) 420-2201 | dicksteinshapiro.com

May 18, 2009

Via E-Mail and First Class Mail

Honorable Kelly Ayotte
Attorney General of New Hampshire
State House Annex
33 Capitol Street
Concord, NH 03301

Re: Batteries.com LLC Server Hacking

Dear General Ayotte:

I am writing to give you notice of a recent data security incident involving our client, Batteries.com LLC, an online merchant, that occurred when an individual or individuals not associated with Batteries.com illegally "hacked" into a Batteries.com server. This hacking resulted in the exposure of name, address and credit card information belonging to a number of Batteries.com customers. Batteries.com has notified law enforcement of the incident and is working with them to identify and prosecute those responsible. Batteries.com also has notified the credit card companies associated with this hacking incident.

The hacking commenced on February 25, 2009 and continued for a period of several weeks. Batteries.com became aware of the hacking beginning in March 2009, after which it began investigating and put in place a series of measures to prevent further risk to customers. Further, Batteries.com retained outside forensic experts to ascertain, in conjunction with internal IT specialists, what happened and which customers may have been affected. The forensic review indicates that the server contained information pertaining to approximately 865 residents of your state.

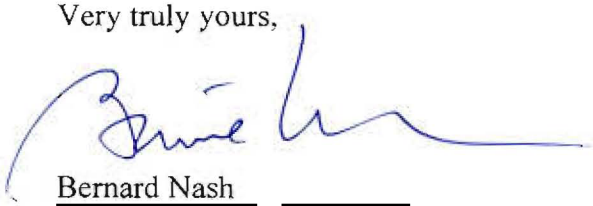
Batteries.com will be notifying those whose information was hacked today and tomorrow. Batteries.com has arranged to provide all affected individuals with two years of credit monitoring and identity theft insurance at the company's expense. Further, Batteries.com has established a call center to support those seeking assistance and created a web site that explains the incident and offers information about privacy and credit protection services. An exemplar copy of the notice letter is enclosed for your information. A handful of Batteries.com customers also have reported unauthorized use of their credit card accounts that is believed to be tied to this hacking. Batteries.com already has provided these individuals with credit monitoring protections and services, as well as providing additional support as needed.

Batteries.com sincerely regrets this incident and is committed to maintaining the confidentiality of its customers' personal information. The company has taken a number of steps to assure the security of data and minimize the likelihood of a similar incident occurring in the future, including limiting the amount of personal information stored, how such information is stored and

the time such information is stored. The company also has put in place enhanced security features to protect its network, and will be unveiling a new website application on June 1, 2009 that adds additional security layers.

Please do not hesitate to contact me if I can provide you with any additional information at any time.

Very truly yours,



Bernard Nash
[redacted]

Enclosure

batteries.com
111 Congressional Blvd. Suite 350, Carmel, IN 46032

May 18, 2009

[Insert Name]
[Insert Address]
[Insert City, State, Zip Code]

Important Security and Protection Notification.
Please read this entire letter.

Dear Valued Customer:

I am personally writing to you as a customer of Batteries.com to alert you of a data security incident which resulted in the unauthorized exposure of your name, address and credit card information to a person or persons not affiliated with Batteries.com.

Law enforcement has been notified of the incident and is investigating. Batteries.com also has notified the credit card companies associated with the exposure. Batteries.com takes this incident seriously and is committed to assuring the security of data and protecting its customers. We encourage you to take advantage of the support services that Batteries.com is offering (described below) to help protect your identity and guard your credit.

The exposure commenced on February 25, 2009 and continued for a period of several weeks when a server belonging to Batteries.com was illegally "hacked." Batteries.com became aware of the exposure beginning in March 2009, after which it began investigating and put in place a series of measures to prevent further exposure of customer information.

Batteries.com has been working with internal and external forensic experts to ascertain what happened and who may have been affected. To date, a handful of Batteries.com customers have reported unauthorized activity regarding their credit card accounts that is believed to be tied to this exposure.

We have modified the computer system where this information was stored and put in place other enhanced security measures as well, including limiting the amount of personal information stored and the time such information is stored. We hope that this letter, and the assistance that we are offering, will answer your questions and provide practical support. We sincerely regret this incident and any concerns it might raise.

What Batteries.com Is Doing to Help Protect Your Privacy and Security

To help protect you from the misuse of your information, Batteries.com is providing you with two years of Experian's Triple Alert℠* product, free of charge. Triple Alert will identify and notify you of key changes in your three national credit reports that may indicate fraudulent activity. Your free two-year membership includes:

- Daily monitoring of all three credit files with Experian, Equifax and Trans Union
- Alerts if key changes are detected on any of your three credit reports
- "No-hit" reports, if applicable, letting you know there were no changes with your credit activity
- Dedicated team of fraud resolution representatives for victims of identity theft
- $25,000 in identity theft insurance provided by Virginia Surety Company, Inc. with no deductible**

*Triple Alert is provided by ConsumerInfo.com, Inc., an Experian company.
**Identity theft insurance coverage is not available for New York residents. Coverage also is unavailable in US overseas Commonwealths or Territories (e.g., Puerto Rico).

We encourage you to activate your free two-year credit monitoring membership quickly. You may activate your membership over the internet or by phone. The deadline for activating your membership is August 15, 2009.

To enroll on-line, visit the following web site and enter your activation code:

Triple Alert Web Site: http://partner.consumerinfo.com/batteries
Your Activation Code: [Activation Code]

If you wish to enroll over the phone for delivery of your membership via US mail, please call 1-888-829-6553.

Please keep in mind that once activated, the code cannot be re-used for another enrollment. The web site will guide you through the process of enrolling in Triple Alert. If you have issues with enrollment on the Triple Alert web site, please call Experian at 1-888-829-6553.

Experian also has set up a Call Center to answer questions you may have and provide you with further assistance and information you may need regarding this incident and the free protections being made available to you. Call Center representatives are available Monday to Friday from 6 a.m. to 6 p.m. and Saturday to Sunday from 8 a.m. to 5 p.m. Pacific Time at 1-888-829-6553.

Further Steps You Can Take to Protect Yourself

In addition to registering for these services, there are additional steps that you can take to help protect yourself from fraud or identity theft.

(1) Review your account statements and credit reports for any suspicious/unauthorized activity and remain vigilant for incidents of fraud and identity theft.

(2) Request a copy of your credit report at *www.annualcreditreport.com*. You are entitled to one free report per year from each of the 3 major credit reporting bureaus:

Credit Bureau	**Credit Report Toll Free No.**	**Website**
Equifax	1-800-685-1111	www.equifax.com
Experian	1-888-397-3742	www.experian.com
TransUnion	1-877-322-8228	www.transunion.com

When you receive your credit reports, review them carefully.

(3) Contact the credit reporting bureau that provided your credit report if you do not understand an item on it. Report any suspected incidents of identity theft to your local police or sheriff's office and the Federal Trade Commission at 1-877-IDTHEFT (438-4338).

(4) Contact one of the 3 major credit reporting bureaus to request that a "fraud alert" be placed on your credit file. A fraud alert indicates to anyone requesting your credit file that you may be a victim of fraud or identity theft. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the creditor should take steps to verify that you have authorized the request. If it cannot, the request should not be satisfied. There is no charge for this service, and it is easy to request. To activate a fraud alert, call any one of the three major credit bureaus listed below. As soon as you alert one credit bureau, it will notify the other two to place fraud alerts on your account

Equifax	Experian	TransUnion
1-888-766-0008	1-888-397-3742	1-800-680-7289
P.O. Box 740241	P.O. Box 9532	P.O. Box 6790
Atlanta, GA 30374-0241	Allen, TX 75013	Fullerton, CA 92834-6790
www.equifax.com	www.experian.com	www.transunion.com

(5) You also may place a security freeze on your credit reports by contacting each of the 3 credit reporting bureaus listed above. A security freeze is designed to prevent potential credit grantors from accessing your credit report for the purpose of opening a new account without your consent. Therefore, using a security freeze may interfere with or delay your ability to obtain credit. The credit reporting bureaus may charge a modest fee (typically from $5-$20) to place a freeze or temporarily or permanently remove a freeze. You should contact the consumer reporting bureaus listed above for additional details on security freezes.

For additional information regarding how you can protect yourself against potential fraud or misuse of your personal information, check the Federal Trade Commission at http://www.ftc.gov/bcp/edu/microsites/idtheft/.

Further, a website has been established at www.batteries.com/security/fraud-prevention.asp to provide you with additional information about this incident and how to protect your identity. We recommend you review this information and consider taking these steps to help guard against potential identity theft.

We sincerely apologize for this incident, regret any inconvenience it may cause you and encourage you to take advantage of the services outlined herein. Should you have questions or concerns regarding this matter and/or the protections available to you, please do not hesitate to contact us.

Sincerely,

Matt Rogers
Managing Director