Buchanan Ingersoll & Rooney PC
Attorneys & Government Relations Professionals

Matthew H. Meade
412 562 5271
matthew.meade@bipc.com

One Oxford Centre
301 Grant Street, 20th Floor
Pittsburgh, PA 15219-1410
T 412 562 8800
F 412 562 1041
www.buchananingersoll.com

February 19, 2014

VIA: U.S. MAIL

Attorney General Joseph Foster
New Hampshire Department of Justice
33 Capitol Street
Concord, NH 03301

Re: DATA SECURITY INCIDENT

Dear Mr. Foster:

I am writing to you on behalf of my client 80sTees.com, Inc. ("80sTees"), a Pennsylvania corporation that specializes in online sales of 80's memorabilia and pop culture gear. 80sTees is providing notice pursuant to N.H. Rev. Stat. Ann. section 359-C:20I(b) of a data security incident. This is a follow-up to the notice I sent on April 3, 2013 which reported that 80sTees would be notifying 14 residents of New Hampshire of a data security incident. Since then 80sTees has learned that the cyber attacker who installed the malware also created a false email address that received the names, addresses, email addresses, phone numbers and credit card information of consumers after they completed credit card purchases on the 80sTees website. After 80sTees sent its original customer notice it received additional complaints of unauthorized use of credit cards. As soon as 80sTees received these complaints it notified the Secret Service. In May 2013, the Secret Service placed a hold on 80sTees' notice letters because the letters could jeopardize its ongoing investigation of the incident. On January 23, 2014, the Secret Service informed 80sTees it had completed its investigation.

Based on what 80sTees has learned, 80sTees has decided to notify every customer who did not already receive notice on April 3, 2013 for the time period from June 3, 2012 until April 30, 2013, including 351 New Hampshire residents, so they can take appropriate action if necessary.

What Happened

On January 29, 2013, Discover Card requested that 80sTees conduct an investigation of its computer system because of some unauthorized charges by Discover customers after completing purchases on its website. Shortly after 80sTees got Discover's request it: (1)

conducted its own investigation including reviewing server log files; (2) recoded its website so that it no longer stored credit card numbers on its server and securely removed all existing credit card data from its server; (3) confirmed that its malware and antivirus scans were operating; (4) reported to the U.S. Secret Service about its investigation; and (5) hired a PCI approved forensic investigator to conduct a full evaluation of its computer server. At that time 80sTees did not find any intrusion or vulnerabilities in 80sTees' server.

On February 27, 2013, 80sTees learned that a small number of Visa customers had also experienced unauthorized charges after a purchase from the 80sTees' website. On March 6, 2013, 80sTees heard from MasterCard that it had concerns about fraudulent credit card charges against cardholders who had placed orders on the 80sTees' website in the 2nd half of 2012. On March 12, 2013, the forensic investigator discovered that 80sTees had been the victim of a cyber attack by a criminal who gained access to and installed malware on its website server sometime in early June 2012 and bypassed its regular antivirus/malware scans.

Beginning on April 3, 2013, 80sTees notified approximately 3,503 customers whose information the credit card companies informed it had been compromised. It is our understanding that the credit card companies had already canceled each of those accounts.

On April 22, 2013, 80sTees received a report from its forensic investigator which indicated that the number of credit cards that had been exposed through the malware was 2,598. On April 30, 2013, 80sTees received calls from two customers who stated that their cards had been compromised after completing transactions in April. 80sTees investigated those customers' complaints and immediately reported them to the Secret Service. The Secret Service then instructed 80sTees not to provide notice to additional customers because it would impact its investigation. During the course of the Secret Service investigation 80sTees learned that the hackers had set up an unauthorized email account that captured its credit card transactions without its knowledge. On January 23, 2014, the Secret Service informed 80sTees that it had completed its investigation and therefore 80sTees was free to provide notice.

What 80sTees is Doing About It

This is a serious matter, and 80sTees has taken aggressive steps to address it and prevent any further unauthorized use of its customer's personal information including the following:

- Stopped accepting credit cards from May 1, 2013 to August 27, 2013;
- On August 27 launched an entirely new website with a new platform and enhanced security, including:
    - Used Cybersource, a company owned by Visa, to securely store and process all credit card details;
    - Tokenization of all credit card data so that even 80sTees.com employees do not have access to customer credit card details.

Tokenization means that once credit card numbers are stored in Cybersource a different number is used to refer to the credit card. The different number cannot be used to make charges to credit cards; and

- Outsourced all website development to a third party that maintains strict version control of all of the code for 80sTees' website, which means that any changes in 80sTees' software that do not match those changes that it knows have been made will throw up a red flag.

- Confirmed that no additional information relating to customer transactions is being sent to the email address set up by the hackers that permitted the unauthorized access;
- Eliminated the storage of customer's credit card numbers on 80sTees' server;
- Continued its investigation of this incident with the assistance of its PCIDSS certified, outside forensic investigator and the federal authorities;
- Increasing the frequency of antivirus and malware scans;
- Continuing to encrypt and protect customer data through secure SSL technology;
- Updating its company policies and procedures on data security and privacy; and
- Conducted mandatory, company-wide data security training in order to increase awareness of data security and privacy.

80sTees notified the 351 New Hampshire residents impacted by this incident via email dated February 12, 2014. A copy of the notice sent to the 351 residents is attached hereto.

Furthermore, 80sTees provided notice to each consumer reporting agency (as defined in 15 U.S.C. 1681a(p)) of this data security incident on February 14, 2014.

Please do not hesitate to contact me at 412 562 5271 if you have questions or concerns.

Very truly yours,

Matthew H. Meade

MHM
Enclosure

230 Westec Dr.
Mt. Pleasant, PA 15666
724-696-5121

Name
Address
City, State ZIP

February , 2014

Re: DATA SECURITY INCIDENT

Dear {Name}:

80sTees.com, Inc. ("80sTees") is notifying you because we have learned that we were the victim of a cyber attack which involved unauthorized access to the credit card information you used to make a purchase on the 80sTees' website. We originally reported this breach in April of 2013 to customers whose credit card numbers had been used fraudulently as reported by the credit card companies to 80sTees. Since then we learned that the scope of the exposure to customer credit card information was even larger than we originally believed. Out of an abundance of caution and even though we are unable to determine whether there was any unauthorized use of your credit card, we are notifying every customer who used a credit card to make a purchase from 80sTees from June 3, 2012 until April 30, 2013 so that you can take appropriate action if you feel it is necessary.

What Happened

On January 29, 2013, Discover Card requested that we conduct an investigation of our computer system because of some unauthorized charges experienced by Discover customers after completing purchases on our website. Shortly after we got Discover's request we: (1) conducted our own investigation including reviewing server log files; (2) recoded our website so that we no longer stored credit card numbers on our server and securely removed all existing credit card data from our server; (3) confirmed that our malware and antivirus scans were operating; (4) reported to the U.S. Secret Service about our investigation; and (5) hired a PCI approved forensic investigator to conduct a full evaluation of our computer server. At that time we did not find any intrusion or vulnerabilities in 80sTees' server.

On February 27, 2013, we learned that a small number of Visa customers had also experienced unauthorized charges after a purchase from the 80sTees' website. On March 6, 2013, we heard from MasterCard that it had concerns about fraudulent credit card charges against cardholders who had placed orders on the 80sTees' website in the 2nd half of 2012. On March 12, 2013, the forensic investigator discovered that 80sTees had been the victim of a cyber attack by a criminal who gained access to and installed malware on our website server sometime in early June 2012 and bypassed our regular antivirus/malware scans.

Beginning on April 3, 2013, we notified approximately 3503 customers whose information the credit card companies informed us had been compromised. It is our understanding that the credit card companies had already canceled each of those accounts.

On April 22, 2013, we received a report from our forensic investigator which indicated that the number of credit cards that had been exposed through the malware was 2,598. On April 30, 2013, we received calls from two customers who stated that their cards had been compromised after completing transactions in April. We investigated those customers' complaints and immediately reported them to the Secret Service. The Secret Service then instructed 80stees not to provide notice to additional customers

because it would impact their investigation. During the course of the Secret Service investigation we learned that the hackers had set up an unauthorized email account that captured our credit card transactions without our knowledge. On January 23, 2014, the Secret Service informed us that it had completed its investigation and therefore 80sTees was free to notify customers about the issue.

Unfortunately the Secret Service was not able to definitively identify the person or persons responsible for the intrusion. Based upon the information that we have learned to date we believe that the hack was originated by a former high level employee who has since died. We do not believe that this incident was in any way connected with the recently publicized hacks involving major U.S. retailers.

What 80sTees is Doing About It

This is a serious matter, and we have taken aggressive steps to address it and prevent any further unauthorized use of your personal information including the following:

- Stopped accepting credit cards from May 1, 2013 to August 27, 2013;
- On August 27 launched an entirely new website with a new platform and enhanced security, including:
  - Used Cybersource, a company owned by Visa, to securely store and process all credit card details;
  - Tokenization of all credit card data so that even 80sTees.com employees, including myself, do not have access to customer credit card details. Tokenization means that once credit card numbers are stored in Cybersource we have a different number that we use to refer to the credit card. The different number cannot be used to make charges to credit cards; and
  - Outsourced all website development to a third party that maintains strict version control of all of the code for our website, which means that any changes in our software that do not match those changes that we know have been made will throw up a red flag.
- Confirmed that no additional information relating to customer transactions is being sent to the email address set up by the hackers that permitted the unauthorized access;
- Eliminated the storage of customers' credit card numbers on our server;
- Continued our investigation of this incident with the assistance of our PCIDSS certified, outside forensic investigator and the federal authorities;
- Increased the frequency of antivirus and malware scans;
- Continuing to encrypt and protect customer data through secure SSL technology;
- Updating our company policies and procedures on data security and privacy; and
- Conducted mandatory, company-wide data security training in order to increase all of our awareness of data security and privacy.

What You Can Do

I recommend that you review your credit card account statements for charges you did not make. If you do not look at your statements every month you should look for unrecognized charges. You should immediately contact your credit card company if you see any unauthorized charges and request that your card be cancelled.

I recommend that you remain vigilant by regularly reviewing your credit reports. Although we did not have your Social Security number you should also be wary of new accounts you did not open and inquiries from creditors that you did not initiate. If you do find suspicious activity on your credit reports or become aware of identity theft, I recommend that you call your local law enforcement office, file a police report of identity theft, and obtain a copy of the police report, as you may need to give copies of the police report to creditors to clear up your records. Even if you do not find any signs of fraud on your reports, you should remain vigilant and check your credit reports regularly.

You may contact the three US credit reporting agencies (Equifax, Experian and TransUnion) to obtain a free credit report from each by calling 1-877-322-8228 or by logging onto www.annualcreditreport.com.

If you would like to place fraud alerts and security freezes on your accounts you can contact Equifax, Experian, Transunion at the numbers listed below:

Equifax	Experian	TransUnion
1-800-685-1111	1-888-397-3742	1-800-888-4213
www.equifax.com	www.experian.com	www.transunion.com

For additional assistance on steps to avoid identity theft or to report an incident of identity theft, or to obtain information about fraud alerts and security freezes write to or call or visit the FTC's website listed below:

Federal Trade Commission
Bureau of Consumer Protection
Division of Privacy and Identity Protection
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580
1-877- IDTHEFT (1-877-438-4338)
http://www.ftc.gov/bcp/edu/microsites/idtheft

As the founder and president of 80sTees I apologize for the inconvenience this incident has caused you. I want to thank you for being a customer of 80sTees. We have let you down and I am embarrassed and angry about that. 80sTees exists to surprise and delight you with a wearable trip down memory lane, not to bring inconvenience into your life. My hope is that by taking the steps listed above we will regain your trust.

Should you have questions or concerns regarding this matter and/or the protections available to you, please do not hesitate to contact me at kevin@80stees.com. You may also call our toll free number at 1-866-807-8337.

Finally, we understand that receiving this letter and discovering this potential issue may bring anger and anxiety into your life. I started 80sTees to bring happiness and fun memories to our customers, so this hits me especially hard. As an apology I would like to offer you 50% off of a single gift certificate valued between $20 and $100. Because our new ecommerce system does not yet have the ability to offer this type of discount you will need to call us and place an order over the phone. Please call us toll free at 1-866-807-8337 and tell us you received a notification about the credit card breach. Please have this email handy so we can mark you off on our list: (INSERT EMAIL HERE). We can then sell you a gift certificate for 50% off with the maximum value being $100.

Sincerely,

Kevin Stecko

Kevin Stecko
President, 80sTees.com, Inc.