McDonald Hopkins
A business advisory and advocacy law firm®

McDonald Hopkins PLC
39533 Woodward Avenue
Suite 318
Bloomfield Hills, MI 48304
P 1.248.646.5070
F 1.248.646.5075

Dominic A. Paluzzi
Direct Dial: 248.220.1356
dpaluzzi@mcdonaldhopkins.com

March 23, 2018

Attorney General Gordon J. MacDonald
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Bigfoot Gun Belts– Incident Notification

Dear Attorney General MacDonald:

McDonald Hopkins PLC represents Bigfoot Gun Belts ("Bigfoot"). I write to provide notification concerning an incident that may affect the security of personal information of thirty-three (33) New Hampshire residents. Bigfoot's investigation is ongoing and this notification will be supplemented with any new significant facts or findings subsequent to this submission, if any. By providing this notice, Bigfoot does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

After identifying suspicious activity within its e-Commerce server on February 1, 2018, Bigfoot immediately engaged external forensic investigators and commenced a prompt and thorough investigation into the incident. As a result of this review, Bigfoot learned that certain customer credit and debit card information may have been obtained by an unauthorized party from its payment portal when purchasing through its online store at www.gunbelts.com, from October 31, 2017 through February 1, 2018. Bigfoot does not store card data on its website; this data was scraped during the transaction. Purchases through its call center were not impacted by this incident and this only impacts Bigfoot Gun Belts products.

Based on Bigfoot's investigation, the information potentially involved in this incident may have included residents' name, credit or debit card number, and card expiration date. The CVV (3 or 4 digit code on the front or back of the card) and debit PIN numbers were not accessed during this incident.

We wanted to make you (and the affected residents) aware of the incident and explain the steps Bigfoot is taking to safeguard the residents against identity fraud. Bigfoot will provide the New Hampshire residents with notice of this incident commencing on March 23, 2018, in substantially the same form as the communication attached hereto. Bigfoot will advise the residents to remain vigilant in reviewing financial and credit card account statements for fraudulent or irregular activity. Bigfoot will provide dedicated call center support to answer questions. Bigfoot will advise the residents about the process for placing a fraud alert on their credit files, placing a security freeze, and obtaining a free credit report. The residents will also be

provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

Since learning of the incident, Bigfoot has implemented enhanced security safeguards to protect from similar intrusions. Bigfoot is also conducting ongoing monitoring of its website and payment portal to ensure that they are secure and cleared of any malicious code.

In addition, we have notified the payment card networks so that they can coordinate with card issuing banks to monitor for fraudulent activity on cards used.

Should you have any questions regarding this notification, please contact me at (248) 220-1356 or dpaluzzi@mcdonaldhopkins.com.

Sincerely,

Dominic A. Paluzzi

DAP/aeh
Enclosure

Return Mail Processing Center
PO Box 6336
Portland, OR 97228-6336

[redacted]

[redacted]

[redacted]

We wanted to make you aware of a recent incident involving potential unauthorized access to some of our customers' card payment data used at *www.gunbelts.com*. The privacy and security of your personal information is of utmost importance to Bigfoot Gun Belts and we are routinely evaluating and improving our security and payment systems to ensure your information is secure.

What Happened?

After identifying suspicious activity within our e-Commerce server on February 1, 2018, we immediately engaged external forensic investigators and commenced a prompt and thorough investigation into the incident. As a result of this review, we learned that certain customer credit and debit card information may have been obtained by an unauthorized party from our payment portal when purchasing through our online store at *www.gunbelts.com*, from October 31, 2017 through February 1, 2018. We do not store card data on our website; this data was scraped during the transaction. Purchases through our call center were not impacted by this incident and this only impacts Bigfoot Gun Belts products.

What Information Was Involved?

Based on our investigation, the information potentially involved in this incident *may* have included your name, credit or debit card number, and card expiration date. The CVV (3 or 4 digit code on the front or back of the card) and debit PIN numbers were not accessed during this incident.

What We Are Doing

Because we value our relationship with you, we wanted to make you aware of the incident, let you know what we are doing to further secure your information, and suggest steps you can take. Since learning of the incident, we have implemented enhanced security safeguards to help protect from similar intrusions. We are also conducting ongoing monitoring of our website and payment portal to ensure that they are secure and cleared of any malicious activity. The payment card networks have also been notified so that they can coordinate with card issuing banks to monitor for fraudulent activity on cards used.

What You Can Do

Below you will find precautionary measures you can take to protect your personal information. Additionally, you should always remain vigilant in reviewing your financial account statements for fraudulent or irregular activity on a regular basis.

As a best practice, you should also call your bank or card issuer if you see any suspicious transactions. The policies of the payment card brands such as Visa, MasterCard, American Express and Discover provide that you are not liable for any unauthorized charges if you report them in a timely manner. You should also ask your bank or card issuer whether a new card should be issued to you.

For More Information

Your trust is sincerely a top priority for Bigfoot Gun Belts, and we deeply regret the inconvenience this may cause. The privacy and protection of our customers' information is a matter we take seriously and we constantly evaluate and improve our payment processes and security systems to ensure the safety of our customers.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at [redacted]. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against misuse of your information. The response line is available Monday through Friday, 6 a.m. to 6 p.m. PST.

We value your business, but beyond your role as a customer we hope to continue to support you as a member of our community.

Sincerely,

Bigfoot Gun Belts

– OTHER IMPORTANT INFORMATION –

You should remain vigilant for incidents of fraud and identity theft by regularly reviewing your account statements and monitoring free credit reports for any unauthorized activity. If you discover any suspicious or unusual activity on your accounts, be sure to report it immediately to your financial institutions, as major credit card companies have rules that restrict them from requiring you to pay for fraudulent charges that are timely reported.

In addition, you may contact the Federal Trade Commission (FTC) or law enforcement, such as your state attorney general, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. You can contact the FTC at:

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
(877) IDTHEFT (438-4338)
https://www.identitytheft.gov/

If you find that your information has been misused, the FTC encourages you to file a complaint with the FTC and to take these additional steps: (1) close the accounts that you have confirmed or believe have been tampered with or opened fraudulently; and (2) file and keep a copy of a local police report as evidence of the identity theft crime.

Obtain Your Credit Report

You should also monitor your credit reports. You may periodically obtain credit reports from each nationwide credit reporting agency. If you discover inaccurate information or a fraudulent transaction on your credit report, you have the right under the federal Fair Credit Reporting Act (FCRA) to request that the credit reporting agency delete that information from your credit report file.

In addition, under the FCRA, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You also may complete the Annual Credit Report Request Form available from the FTC at https://www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf, and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You may also contact any of the three major credit reporting agencies to request a copy of your credit report.

Place a Fraud Alert or Security Freeze on Your Credit Report File

In addition, you may obtain information from the FTC and the credit reporting agencies about fraud alerts and security freezes. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you, but it also may delay your ability to obtain credit. If you suspect you may be a victim of identity theft, you may place a fraud alert in your file by calling just one of the three nationwide credit reporting agencies listed below. As soon as that agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file. An initial fraud alert will last 90 days. An extended alert stays on your file for seven years. To place either of these alerts, a consumer reporting agency will require you to provide appropriate proof of your identity, which may include your Social Security number. If you ask for an extended alert, you will have to provide an identity theft report.

Also, you can contact the nationwide credit reporting agencies regarding if and how you may place a security freeze on your credit report. A security freeze prohibits a credit reporting agency from releasing information from your credit report without your prior written authorization, which makes it more difficult for unauthorized parties to open new accounts in your name. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. The credit reporting agencies have 3 business days after receiving a request to place a security freeze on a consumer's credit report. You may be charged to place or lift a security freeze. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.

You may contact the nationwide credit reporting agencies at:

Equifax	**Experian**	**TransUnion**
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
(800) 525-6285	(888) 397-3742	(800) 680-7289
www.equifax.com	www.experian.com	www.transunion.com

Iowa Residents: You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity Theft: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, Telephone: (515) 281-5164

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Department of Justice, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 877-566-7226.

Oregon Residents: You may obtain information about preventing identity theft from the Oregon Attorney General's Office: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392