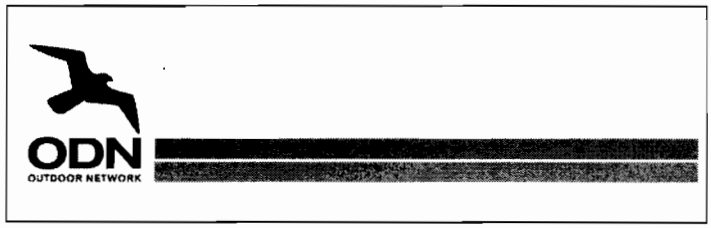

Outdoor Network LLC
730 US 27 North
Lake Placid, FL 33852
229-299-9565 ext. 432
security@outdoornetwork.com

September 6, 2013

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

RE: Breach of Security Involving Computerized Data

Dear Attorney General Foster:

Pursuant to N.H. Rev. Stat. §§ 359-C:19 *et seq.*, I am writing to notify you of possible unauthorized access of personal information on our websites, boats.net and partzilla.com. The incident is believed to involve approximately 600 of our New Hampshire customers.

On July 16, 2013, we identified what appeared to be malware inserted by unauthorized third parties into the shopping cart portions of our websites. The malware appears to have targeted transactions by customers that made purchases on our websites using a credit card between December 2012 and July 2013. The malware may have collected the following personal information from affected customers: name, address, credit card number, card expiration date and card security code (CVV or CVC code).

Upon learning of the incident, we immediately took steps to notify all potentially affected credit card companies so they could take necessary action to protect individual card holders. Additionally, we undertook a formal, independent PCI Forensic Investigation of our network which has confirmed that the malware was contained and eliminated, and that the integrity of our online checkout systems has been fully restored.

We intend to send letters to potentially affected New Hampshire residents notifying them about this incident during the week of September 9, 2013. A sample of the notice letter is enclosed. Please contact me with any questions or concerns regarding this incident.

Sincerely,

Martin Polo, CEO

ICO - G. LUIS ALDAY, CPA, P.A.
3748 SW 30th Avenue
Hollywood, Florida 33312

September 11, 2013

Sample A. Sample
123 Anystreet 000001
Anytown, US 12345-6789

Dear Sample A. Sample:

We are strongly committed to the security of our customers' information and strive to let you know about security concerns as soon as possible. We recently learned of an incident on our websites (boats.net and partzilla.com) that may have exposed your personal information to unauthorized persons.

We believe the incident occurred when unauthorized third parties compromised and inserted malware into the shopping cart portions of our websites. The malware appears to have targeted transactions by customers that made purchases on our websites using a credit card between December 2012 and July 2013. You are receiving this notice because our records indicate you made a credit card purchase on one of the above websites during this time period. The malware may have collected the following personal information from affected customers: name, address, credit card number, card expiration date and card security code (CVV or CVC code).

Upon learning of the incident, we immediately took steps to notify all potentially affected credit card companies so they can take any actions necessary to protect your credit card account. You can take the following additional precautionary steps to further protect yourself.

- **Remain vigilant** – We encourage you to remain vigilant by reviewing your account statements and free credit reports.
    - If you discover errors or suspicious activity on your credit card account, you should immediately contact the credit card company and inform them that you have received this letter. Confirm the address they have on file for you is your current address, and that all charges on the account are legitimate.
    - To obtain an annual free copy of your credit reports, visit www.annualcreditreport.com or call 1-877-322-8228. Review your credit reports carefully for inquiries from companies you did not contact, accounts you did not open or debts on your accounts that you do not recognize. Also make sure to verify the accuracy of your Social Security Number, address(es), complete name and employer(s) information. If information on a report is incorrect, notify the credit bureau directly using the telephone number on the report. Additional contact information for the major credit bureaus is as follows:

Equifax:	Experian:	TransUnion:
P.O. Box 740241	P.O. Box 2104	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19022
1-800-685-1111	1-888-397-3742	1-800-916-8800
www.equifax.com	www.experian.com	www.transunion.com

- **Consider placing a fraud alert or security freeze on your credit file** – Credit bureaus have tools you can use to protect your credit, including fraud alerts and security freezes.

    - A fraud alert is a cautionary flag, which is placed on your credit file to notify lenders and others that they should take special precautions to ensure your identity before extending credit. Although this may cause some short delay if you are the one applying for credit, it might protect against someone else obtaining credit in your name. Call any one of the three credit reporting agencies at the numbers below to place fraud alerts with all three of the agencies.

Equifax:	Experian:	TransUnion:
1-888-766-0008	1-888-397-3742	1-800-680-7289

    - A security freeze is a more dramatic step that will prevent lenders and others from accessing your credit report entirely, which will prevent them from extending credit. With a security freeze in place, even you will need to take special steps when applying for credit. A security freeze may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services. A security freeze will need to be obtained separately from each credit reporting agency. You must contact each credit agency separately to order a security freeze. You can obtain more information by visiting the credit bureaus at the following addresses.

    Equifax – https://www.freeze.equifax.com/Freeze/jsp/SFF_PersonalIDInfo.jsp
    Experian – http://www.experian.com/consumer/security_freeze.html
    TransUnion – http://www.transunion.com/personal-credit/credit-disputes/credit-freezes.page

- **Report suspicious activity** – If you believe you are the victim of fraud or identity theft, file a police report and get a copy of the report to submit to your creditors and others that may require proof of a crime to clear up your records. The report may also provide you with access to services that are free to identity theft victims.

* * *

Protecting the privacy of your personal information is important to us, and we regret any inconvenience this incident may cause you. To better address your concerns, we have hired ConsumerInfo.com, Inc., an Experian company, to provide certain notification and call center related services. Should you have any questions, please call our customer care center toll free at 888-829-6550 and a representative will be happy to assist you.

Martin Polo

CEO – Outdoor Network LLC