FREEMAN MATHIS & GARY
A LIMITED LIABILITY PARTNERSHIP

100 Galleria Parkway
Suite 1600
Atlanta, Ga. 30339-5948

Tel: 770.818.0000
Fax: 770.937.9960

www.fmglaw.com

David A. Cole
Partner

Writer's Direct Access
770.818.1287

dcole@fmglaw.com

July 16, 2018

VIA U.S. MAIL & EMAIL

New Hampshire Department of Justice
Office of the Attorney General
33 Capitol Street
Concord, NH 03301
attorneygeneral@doj.nh.gov

Re: Notice of Breach in the Security of Personal Information

Dear Attorney General:

I represent EBSCO Sign Group, Inc. ("EBSCO") which owns and operates the website www.outdoorsignsamerica.com. This letter is being provided pursuant to N.H. Rev. Stat. § 359-C:20, which requires that your office be notified in the event of a breach in the security of confidential personal information affecting New Hampshire residents.

EBSCO recently learned that a malware intrusion affected the e-commerce platform on its website, www.outdoorsignsamerica.com, between the dates of September 12, 2017 and May 18, 2018. Its investigation indicates that the malware intercepted payment card and contact information that was entered by customers on the shopping cart checkout page and then transmitted that information to an unknown, outside email account. EBSCO believes the malware affected purchases made on outdoorsignsamerica.com between the dates of September 12, 2017 and May 18, 2018, and may have provided an unauthorized person access to customers' names, billing addresses, email addresses, credit or debit card numbers, CVV numbers, and expiration dates. No other customer personal information, such as Social Security numbers, dates of birth, driver's license numbers, or government identification numbers, was impacted by this incident because EBSCO does not collect that information on its website.

In compliance with all legal obligations, EBSCO is providing written notice to all individuals who made a purchase on the website during that time about this issue. A sample copy of the notice being mailed on July 16, 2018 is enclosed for your reference. In total, EBSCO believes this incident affected 871 individuals affected by this incident, which included 5 residents of New Hampshire.

Please know that EBSCO takes the protection of its customers' information seriously and is taking steps to continue investigating this incident, help mitigate the potential for harm, and prevent this from happening again. Upon discovering the malware, EBSCO turned off the shopping cart feature on the website while it conducted a thorough review of the website and its ecommerce platform with legal counsel and cybersecurity experts. EBSCO is confident that it has removed the malware and secured the website and, as a result, it has now reopened the shopping cart for transactions. EBSCO also has notified law enforcement and the credit card companies about the incident, and is cooperating with their investigations. In addition, as discussed above, EBSCO worked diligently to directly notify all customers affected by this incident.

I believe this provides you with all information necessary for your purposes and to comply with New Hampshire law. However, if you have any additional questions or need further information, please contact me.

Very truly yours,

FREEMAN MATHIS & GARY, LLP

David Cole

DAC/jmr
Enclosure

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

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Notice of Data Breach

Dear <<Name 1>>:

We are writing to notify you of a data security incident that occurred on the website outdoorsignsamerica.com and which may have involved your personal information. Please read this letter carefully.

What Happened

We have recently learned that a malware intrusion affected the e-commerce platform on our website, outdoorsignsamerica.com, between the dates of September 12, 2017 and May 18, 2018. Our investigation indicates that the malware intercepted payment card and contact information that was entered by customers on the shopping cart checkout page and then transmitted that information to an unknown, outside email account. Promptly after discovering the malware, we shut down the shopping cart, conducted an in-depth investigation, and engaged outside cybersecurity experts to determine the facts. We are confident that we have now removed the malware and secured the website, so we have now reactivated the website's shopping cart.

What Information was Involved

We believe the malware affected all purchases made on outdoorsignsamerica.com between the dates of September 12, 2017 and May 18, 2018. You are receiving this letter because our records indicate that you made a purchase on the website during that time. As a result, we believe the malware may have provided an unauthorized person access to your name, billing address, email address, credit or debit card number, CVV number, and expiration date. No other customer personal information, such as Social Security numbers, dates of birth, driver's license numbers, or government identification numbers, was impacted by this incident because we do not collect that information on the website.

What We Are Doing

Please know that we take the protection of our customers' personal information seriously and we are taking steps to help mitigate the potential for harm and prevent future incidents. As part of our investigation of this incident, we conducted a thorough review of the website and its ecommerce platform. We are confident that we have removed the malware and secured the website and, as a result, we have now reopened the shopping cart for transactions. We also have notified law enforcement and the credit card companies about the incident, and we are cooperating with their investigations. In addition, we have worked diligently to directly notify customers who have been affected by this incident.

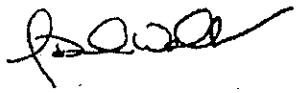
What You Can Do

We recommend that you remain vigilant by reviewing and monitoring your account statements and credit reports to detect any errors or unauthorized activity. If you discover any errors or unauthorized activity, you should contact your financial institution or call the number on the back of your payment card. You also may file a report with law enforcement, your state attorney general, and/or the Federal Trade Commission. In addition, please refer to the enclosed documentation which contains additional steps you may take to protect your information from misuse.

For More Information

We are very sorry for any concern or inconvenience this incident has caused or may cause you. If you have any other questions or concerns that you would like to discuss, please contact our dedicated, incident response hotline at 877-797-6091 between the hours of 6:00 a.m. and 6:00 p.m. Pacific Time, Monday through Friday.

Sincerely,



David Walker
Vice President

Recommended Steps to Help Protect Your Information

1. **Review personal account statements and credit reports.** We recommend that you remain vigilant by reviewing personal account statements and monitoring credit reports to detect any errors or unauthorized activity. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call (877) 322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months. If you discover any suspicious items, you should report any incorrect information on your report to the credit reporting agency. The names and contact information for the credit reporting agencies are:

Equifax	Experian	TransUnion
1-866-766-0008	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
www.equifax.com	www.experian.com	www.transunion.com

2. **Report suspected fraud.** You have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You should report suspected incidents of identity theft to local law enforcement, your state's Attorney General, and/or the Federal Trade Commission.

3. **Place Fraud Alerts** with the three credit reporting agencies listed above. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. Please note that it is only necessary to contact one of the credit reporting agencies and use only one of these methods. As soon as one of the three agencies confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports for your review.

4. **Place a Security Freeze.** By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above in writing to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. The cost of placing the freeze varies by the state you live in and for each credit reporting agency. The credit reporting agency may charge a fee of up to $5.00 to place a freeze, lift, or remove a freeze. However, if you are a victim of identity theft and have filed a report with your local law enforcement agency or submitted an ID Theft Complaint Form with the Federal Trade Commission, there may be no charge to place the freeze.

5. **Obtain additional information** about the steps you can take to avoid identity theft from the following agencies:

   - **California Residents:** Visit the California Office of Privacy Protection, www.privacy.ca.gov, for additional information on protection against identity theft.
   - **Iowa Residents:** Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, (515) 281-5164.
   - **Kentucky Residents:** Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, (502) 696-5300.
   - **Maryland Residents:** Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, (888) 743-0023.
   - **Massachusetts:** Office of the Attorney General, One Ashburton Place, Boston, MA 02108-1518, https://www.mass.gov/orgs/office-of-attorney-general-maura-healey, (617) 727-2200.
   - **North Carolina Residents:** Office of the Attorney General of North Carolina, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.com, (919) 716-6400.

- **Oregon Residents:** Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us, (877) 877-9392.

- **Rhode Island Residents:** Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, (401) 274-4400.

- **All US Residents:** Federal Trade Commission, Bureay of Consumer Protection, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.ftc.gov/idtheft, 1-877-IDTHEFT (438-4338).

6. **Summary of Rights Under the Fair Credit Reporting Act.** The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. You have certain rights under the FCRA, including: (1) You must be told if information in your file has been used against you; (2) You have the right to know what is in your file (you "file disclosure"); (3) You have the right to ask for a credit score; (4) You have the right to dispute incomplete or inaccurate information; (5) Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; (6) Consumer reporting agencies may not report outdated negative information; (7) Access to your file is limited to people with a valid need; (8) You must give your consent for reports to be provided to employers; (9) You may limit "prescreened" offers of credit and insurance you get based on information in your credit report; (10) You may seek damages from violators; and (11) identity theft victims and active duty military personnel have additional rights. For more information, visit www.ftc.gov/credit. States may enforce the FCRA, and many states have their own consumer reporting laws. In some cases, you may have more rights under state law. For more information, contact your state or local consumer protection agency or your state Attorney General.