AirBorn

June 13, 2014

The Honorable Joseph Foster
Office of the Attorney General
Department of Justice
33 Capitol Street
Concord, NH 03301

Re: Notice of computer security incident

Dear Attorney General Foster:

I write on behalf of AirBorn, Inc. to inform you of a computer security incident that affected one (1) New Hampshire resident.

We believe the incident occurred on or about May 28, 2014, when an unknown individual, without authorization and using a stolen password, accessed the e-mail account of a person who was performing consulting services for AirBorn. It is possible that the password used to access the e-mail account was stolen a few days before that date. The password for the affected e-mail account was promptly changed to re-secure the account. On May 29, 2014, AirBorn discovered that the incident may have compromised personal information of its employees.

In particular, one of the messages in the e-mail account contained AirBorn employee stock ownership plan information, including Social Security numbers, contribution and compensation data, employment status, and, for a limited number of individuals, address information. We have not been able to determine whether the e-mail message at issue was actually accessed by the intruder.

Notification letters are being sent today to affected individuals, including the affected New Hampshire resident. A sample copy of the notification letter is attached for your convenience. We have also arranged to have AllClear ID provide identity protection services to affected individuals for the next twelve (12) months at no cost to the individuals.

We are in touch with law enforcement and are continuing to investigate the incident. We are also reporting the incident to federal authorities via publicly-available reporting tools. Law enforcement has not requested that we delay notification concerning the incident.

Please do not hesitate to contact us should you need any additional information.

Sincerely,

Cindy Lewis
Chief Executive Officer
AirBorn, Inc.
LewisC@airborn.com
3500 AirBorn Circle
Georgetown, TX 78626
Phone: 512-864-6472

Encl.

AirBorn, Inc. c/o AllClear ID, Inc. · P.O. Box 3825 · Suwanee, GA 30024

John Q. Sample
[ADDRESS]
[ADDRESS]
[CITY, STATE, ZIP]

June 13, 2014

Dear John Q. Sample,

Re: Computer security incident

I am writing on behalf of AirBorn, Inc. to inform you of a computer security incident which may have resulted in the compromise of your personal information. We believe the incident occurred on or about May 28, 2014, when an unknown individual accessed an e-mail account without authorization using a stolen password. One of the messages in the e-mail account contained AirBorn employee stock ownership plan information, including Social Security numbers, contribution and compensation data, employment status, and, for a limited number of individuals, address information. Although we have not been able to determine whether that particular e-mail message was accessed by the intruder, we are encouraging you to make use of the identity protection services we are offering at no cost to you, as described below.

We have arranged to have AllClear ID protect your identity for 12 months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 12 months:

AllClear SECURE: The team at AllClear ID is ready and standing by if you need help protecting your identity. This protection is automatically available to you with no enrollment required. If a problem arises, simply call 1-866-979-2512 and a dedicated investigator will do the work to recover financial losses, restore your credit and make sure your identity is returned to its proper condition. AllClear maintains an A+ rating at the Better Business Bureau.

AllClear PRO: This service offers additional layers of protection including triple bureau credit monitoring and a $1 million identity theft insurance policy. To use the PRO service, you will need to enroll and provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com or by phone by calling 1-866-979-2512 using the following redemption code: 9999999999.

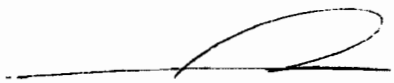
Please note that additional steps may be required by you in order to activate your phone alerts and monitoring options.

Regardless of whether you utilize these identity protection services, we encourage you to be vigilant, including by reviewing your account statements and monitoring free credit reports. For additional information, please see the enclosed sheet titled "Information about Identity Theft Prevention" and the enclosed "Frequently Asked Questions" document, or call 1-866-979-2512.

We are in touch with law enforcement and are continuing to investigate the incident; however, law enforcement has not requested that we delay this notification to you. We are taking this opportunity to review our information security practices and to reinforce policies associated with the secure use of authentication credentials and the secure use of e-mail.

The protection of personal information is very important to AirBorn. We sincerely apologize for any inconvenience this incident may have caused.

Sincerely,



Cindy Lewis
Chief Executive Officer
AirBorn, Inc.

Information about Identity Theft Prevention

You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax, P.O. Box 105139, Atlanta, Georgia 30374-0241, 1-800-685-1111, www.equifax.com
Experian, P.O. Box 2002, Allen, TX 75013, 1-888-397-3742, www.experian.com
TransUnion, P.O. Box 6790, Fullerton, CA 92834-6790, 1-800-916-8800, www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding identity theft.

Federal Trade Commission, Consumer Response Center
600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

Fraud Alerts: There are also two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by calling the toll-free fraud number of any of the three national credit reporting agencies listed below.

Equifax: 1-800-525-6285, www.equifax.com
Experian: 1-888-397-3742, www.experian.com
TransUnion: 1-800-680-7289, www.transunion.com

Credit Freezes: You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally $5 to $20 per action at each credit reporting company. *Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.* Since the

instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax, P.O. Box 105788, Atlanta, GA 30348, www.equifax.com
Experian, P.O. Box 9554, Allen, TX 75013, www.experian.com
TransUnion, LLC, P.O. Box 2000, Chester, PA, 19022-2000, www.transunion.com

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed above.

Frequently Asked Questions

Q: I received a letter that my personal information may have been compromised. Is this letter legitimate? Why did I get this letter?

A: Yes, the letter is legitimate. AirBorn is sending the letter in order to inform you that an e-mail message containing some personal information concerning you may have been accessed by an unauthorized individual.

Q: What happened?

A: We believe an unknown individual used a stolen password to gain access to the e-mail account of an individual who was performing consulting services for the company's employee stock ownership plan. One of the messages in that e-mail account contained employee stock ownership plan information.

Q: What personal information may have been compromised?

A: The e-mail message contained Social Security numbers, contribution and compensation data, and employment status for a number of participants in the company's employee stock ownership plan. For a limited number of those individuals, mailing address information was also included.

Q: Are you sure that the e-mail message containing personal information was actually accessed or reviewed by an unauthorized individual?

A: No. We are not able to determine if that e-mail message was accessed by the intruder; we only know that the intruder could have accessed the e-mail message.

Q: Are you aware of any wrongful use of my personal information?

A: No. AirBorn has not learned of any wrongful use of the personal information contained in the e-mail message. We will continue to monitor the situation. We take our obligation to help you protect your information very seriously, and deeply regret that this has happened.

Q: Are you offering identity theft protection and credit monitoring?

A: Yes. We have arranged to have AllClear ID protect your identity for 12 months at no cost to you. The details are set forth in the letter you received.

Q: When did this incident occur?

A: It appears that the e-mail account was first used without authorization on May 28, 2014, although it is possible that the e-mail account password may have been stolen a few days before that. The password for the affected e-mail account was promptly changed later that same day (i.e, on May 28, 2014), to re-secure the account. On May 29, 2014, AirBorn learned that personal information may have been compromised.

Q: Why is there a delay between the incident and notifying me that this happened?

A: After learning that the incident occurred, AirBorn performed an investigation to determine the scope of the incident and to compile information about individuals whose information may have been involved.

AirBorn also took steps to comply with applicable state laws and made arrangements for identity protection services and notification services.

Q: What is AirBorn doing to keep this from happening again?

A: We are taking this opportunity to review our information security practices and to reinforce policies associated with the secure use of authentication credentials and the secure use of e-mail.

Q: Are you working with law enforcement?

A: Yes, we are in touch with law enforcement and are continuing to investigate. We are also reporting the incident to federal authorities via publicly-available reporting tools.