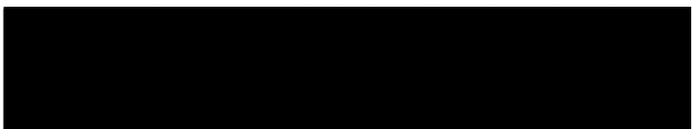




April 7, 2015



Attorney General Joseph Foster
New Hampshire Department of Justice
Attn: Data Security Breach
33 Capitol Street
Concord, NH 03301

STATE OF NH
DEPT OF JUSTICE
2015 APR 10 PM 12:22

Re: Suspected Data Security Breach Notification - Austin Powder

Dear Mr. Foster:

I am writing in connection with N.J. STAT. § 359-C:20 on behalf of my client, Austin Powder Company. Anthem, Inc. ("Anthem") is the third-party administrator for the Austin Powder Company Comprehensive Welfare Plan. As you are likely aware, Anthem recently experienced a data security breach. Based on our investigation, we have determined the breach may have compromised the personal information of certain New Hampshire residents.

It is our understanding that on January 29, 2015, Anthem determined it was the victim of a cyber-attack. Through its investigation, Anthem learned that cyber attackers executed a sophisticated attack over the course of several weeks, beginning in early December 2014, to gain unauthorized access to information stored in Anthem's IT system. The information accessed includes individuals' personal information such as names, dates of birth, Social Security numbers, health care ID numbers, home addresses, email addresses, and employment information, including income data. Based on the information we have now, it is our understanding that no credit card or banking information was compromised. There is also no evidence that medical information such as claims, test results, or diagnostic codes was obtained.

Austin Powder first learned of the breach on February 5, 2015, and has been working with Anthem to gather information and ensure this issue is properly addressed. It is our understanding that as soon as Anthem discovered the attack, Anthem immediately began working to close any security vulnerability, contacted the FBI, and has been cooperating with the FBI's investigation. Anthem also retained Mandiant, one of the world's leading cybersecurity firms, to assist with the investigation and to strengthen the security of its systems. We will continue to work with Anthem to ensure it takes all necessary steps to investigate and address this incident.

Based on our investigation and the information Anthem has provided to date, we believe that thirty-four (34) New Hampshire residents who provided Austin Powder with personally identifiable information in connection with the Austin Powder Company Comprehensive Welfare Plan were potentially affected.

It is also our understanding that Anthem already provided notice of this breach to your office (a copy of the notice is attached) and is in the process of coordinating the distribution of notifications to New Hampshire residents, if it has not done so already. To ensure Austin Powder fulfills its notification requirements, a copy of the attached notice will be mailed to potentially affected New Hampshire residents as well on or about April 7, 2015.

If you have any questions, please do not hesitate to contact me.

Very Truly Yours,

TUCKER ELLIS LLP

Ann M. Caresani

Ann M. Caresani



February 6, 2015

New Hampshire Department of Justice
33 Capitol St.
Concord, NH 03301

To Whom It May Concern:

Pursuant to N.H. Rev. Stat. Ann. 359-C:19 – 359-C:21, this is to notify you that on December 10, 2014, Anthem, Inc. was the victim of a cyber-attack.

On January 27, 2015, Anthem discovered that one of its database warehouses was experiencing a suspicious data query. We immediately stopped the query and launched an internal investigation. On January 29, 2015, we determined that we were the victim of a sophisticated cyber-attack. We notified federal law enforcement officials and shared the indicators of compromise with the HITRUST C3 (Cyber Threat Intelligence and Incident Coordination Center).

Our investigation shows the attacker had a proficient understanding of the data platforms and successfully utilized valid illegally-obtained database administrator logon information. Through our investigation, Anthem was able to rule out any internal resources as the source of the data breach. We continue working with federal investigators to determine who is responsible and why Anthem, Inc. was targeted.

At this time, we are conducting a thorough IT forensic investigation to determine whose information was accessed. This incident affects members and groups whose data was contained in the database warehouse during the time of the data queries – December 10, 2014 – January 27, 2015. Specific numbers of impacted New Hampshire residents will be provided when that information has been identified and confirmed.

Our investigation to date indicates that the information accessed included names, dates of birth, social security numbers, street addresses, email addresses and employment information. We are working to determine whose social security numbers were accessed. Currently, there is no indication that the information accessed included credit card information/financial information or medical history information.

We are not aware of any fraud that has occurred as a result of this incident against our members.

Anthem has contracted with Mandiant – a global company specializing in the investigation and resolution of cyber-attacks. Anthem will work with Mandiant to ensure there are no further vulnerabilities and work to strengthen security. Additionally, Anthem has changed passwords and secured the compromised database warehouse.

For more information, please email Privacy_Incident-sm@anthem.com.

Sincerely,

Anthem, Inc.

Dear _____,

We are writing to notify you that as a result of actions taken by an unauthorized party, information you previously provided to Austin Powder Company or Anthem, Inc. ("Anthem") may have been compromised. Anthem, Inc., the third-party administrator for the Austin Powder Company Comprehensive Welfare Plan, has informed us that on January 29, 2015, it discovered that cyber attackers executed a sophisticated attack over the course of several weeks, beginning in early December 2014, to gain unauthorized access to information stored in Anthem's IT system. The information accessed includes individuals' personal information such as names, dates of birth, Social Security numbers, health care ID numbers, home addresses, email addresses and employment information, including income data. Based on the information we have now, it is our understanding that no credit card or banking information was compromised. There is also no evidence that medical information such as claims, test results, or diagnostic codes was obtained.

We first learned of the breach on February 5, 2015 and have been working with Anthem to gather information and ensure this issue is properly addressed. It is our understanding that as soon as Anthem discovered the attack, Anthem immediately began working to close any security vulnerability, contacted the FBI, and has been cooperating with the FBI's investigation. Anthem also retained Mandiant, one of the world's leading cybersecurity firms, to assist with the investigation and to strengthen the security of its systems. We will continue to work with Anthem to ensure it takes all necessary steps to investigate and address this incident.

If you have any questions regarding the incident or the contents of this letter, you can contact Carol Sedlako, Benefits Manager, Austin Powder Company, 25800 Science Park Drive, Cleveland, OH 44122, (216) 839-5428.

We also want to make you aware of important steps you can take to protect yourself against identify theft and fraud. We recommend that you regularly review your credit and debit card account statements to determine if there has been any unauthorized activity. If you notice any unusual activity, you should contact the bank that issued the debit or credit card immediately.

In addition, you are entitled to obtain a free copy of your credit report once a year. A credit report contains important information about your credit history and the status of your credit accounts. You can obtain a copy of your credit report by contacting one of the following national consumer reporting agencies:

Equifax
P.O. Box 740241
Atlanta, GA 30374-0241
800-525-6285
www.equifax.com

Experian
P.O. Box 2002
Allen, TX 75013
888-397-3742
www.experian.com

TransUnion
P.O. Box 105281
Atlanta, GA 30348-5281
877-322-8228
www.transunion.com

In order to further protect yourself, you may also want to consider placing either a fraud alert or security freeze on your credit file. A **FRAUD ALERT** indicates to anyone requesting

your credit file that you suspect you are a victim of fraud. A fraud alert does not affect your ability to get a loan or credit. Instead, it alerts a business that your personal information might have been compromised and requires the business to verify your identity before issuing you 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. A **SECURITY FREEZE** prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. Please be aware, however, 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. You can obtain additional information about fraud alerts and security freezes, including any fees you may be required to pay in order to place a fraud alert or security freeze on your credit file, by contacting the credit reporting agencies listed above or the Federal Trade Commission, whose contact information is listed below.

If you notice any suspicious activity with your accounts or suspect you are the victim of identity theft, you have the right to and should report the incident to your local law enforcement office, the Florida Attorney General and/or the Federal Trade Commission. The contact information for the Federal Trade Commission is:

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

For Maryland residents: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General at:

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place, 16th Floor
Baltimore, MD 21202
1-888-743-0023
www.oag.state.md.us

For North Carolina residents: You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office at:

North Carolina Attorney General's Office
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
1-877-566-7226
www.ncdoj.gov

For Massachusetts residents: Under Massachusetts law, you have the right to obtain a police report in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

It is our understanding that Anthem intends to prepare and distribute notices regarding this incident, and may have done so already. If you receive a notice from Anthem, please review it carefully as it may contain, among other things, additional information about the incident and information for third-party identity protection services, which Anthem may provide affected individuals at no cost.

We sincerely apologize for any inconvenience you may experience as a result of this incident.

Sincerely,