VARNUM
ATTORNEYS AT LAW

Bridgewater Place • Post Office Box 352
Grand Rapids, Michigan 49501-0352
Telephone 616 / 336-6000 • Fax 616 / 336-7000 • www.varnumlaw.com

Timothy E. Eagle

Direct: 616 / 336-6537
teeagle@varnumlaw.com

June 6, 2017

Attorney General Bob Ferguson
Consumer Protection Division
800 5th Ave, Suite 2000
Seattle, WA 98104-3188

Re: Notice of Data Breach

Dear Attorney General Ferguson:

Pursuant to Rev. Code. Wa Ann. § 19.255.010 (10), we are writing to notify you of a breach of security involving approximately 78 Washington residents. This letter is to provide notification on behalf of our client, Airway Oxygen, Inc., a Michigan corporation, that its computer system suffered a "ransomware" attack on April 18, 2017. Our client's records indicate that 78 persons are Washington residents having personal information which may have been on the computer system. Our client has no indication that any of the personal information stored on the computer network was accessed and/or acquired. Nevertheless, our client wanted to provide notice of the situation.

On the evening of April 18, 2017, our client learned that unidentified criminal(s) had installed ransomware in order to deny the company access to the data on the computer system. Since learning of the incident, our client immediately took steps to secure the internal system against further intrusion, including by scanning the entire internal system, changing passwords for users, vendor accounts and applications, conducting a firewall review, updating and deploying security tools, and installing software to monitor and issue alerts as to suspicious firewall log activity. Our client also reported the incident to the FBI and is cooperating with its efforts. Our client also hired a cyber-security firm to assist in conducting an investigation to assess the cause and impact of the breach.

Our client's records indicate that 78 Washington residents are persons having on the computer system personal information related to the provision by Airway Oxygen, Inc. of medical equipment or supplies, namely information which may have included, full name, home address, Airway account number, birth date, social security number, diagnosis, medical equipment or supplies furnished by Airway Oxygen, health insurance carrier and policy information and billing and payment histories with Airway Oxygen. Pursuant to Rev. Code. Wa Ann. § 19.255.010 (10), written notice is being provided to those Washington residents under the notice requirements and timeline established by federal HIPPA guidelines. Template copies of the proposed notices are attached hereto.

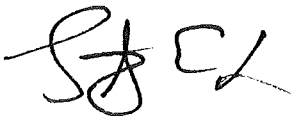
VARNUM
ATTORNEYS AT LAW

If you have any questions or need any help with anything mentioned in this letter, please contact me by e-mail at teeagle@varnumlaw.com or by phone at 616.336.6537.

Our client takes seriously its role in maintaining the security of all individuals' information. Please know that our client is taking steps, including the procedural changes noted above, to reduce the risk of this happening again.

Sincerely yours,

VARNUM



Timothy E. Eagle

TEE/bms

11883697_1.docx

Enclosure

AIRWAY OXYGEN INC.
PO Box 9410
Wyoming, MI 49509

June [ ], 2017

[FName] [LName]
[Address1]
[Address 2]
[City], [State] [Zip]

Re: Notice of Data Breach

Dear [FName]:

We are sending this letter to you to inform you of a recent incident involving your personal information.

WHAT HAPPENED?

On the evening of April 18, 2017, we learned that unidentified criminal(s) had gained access to our technical infrastructure and installed ransomware in order to deny Airway Oxygen Inc. access to its own data. Ransomware is a type of malware that attempts to deny access to a user's data by encrypting data. Our records indicate that your protected health information was on the computer network. We have no indication that any of your protected health information stored on the computer network was accessed and acquired. Nevertheless, we wanted to provide notice to you so that you would be aware of the situation.

We truly regret that this incident has occurred and apologize for any difficulty or inconvenience it may cause you.

WHAT INFORMATION WAS INVOLVED?

The types of protected health information that were involved in the breach include some or all of the following data regarding our customer/end users and payment sources: full name, home address, birth date, telephone number, diagnosis, the type of service we are providing you, and health insurance policy numbers. No bank account numbers or debit or credit card numbers were exposed in the breach.

YOUR SOCIAL SECURITY NUMBER WAS NOT INVOLVED IN THE BREACH.

WHAT WE ARE DOING

Since learning of the incident, we immediately took steps to secure our internal systems against further intrusion, including by scanning the entire internal system, changing passwords for users, vendor accounts and applications, conducting a firewall review, updating and deploying security tools, and installing software to monitor and issue alerts as to suspicious firewall log activity. We have reported the incident to the FBI and will cooperate with their efforts. We have hired a cyber-security firm to assist in

conducting an investigation to assess the cause and impact of the breach. In addition, we are identifying further actions to reduce the risk of this situation recurring.

WHAT YOU CAN DO

We are keenly aware of how important your protected health information is to you.

As a security precaution, we recommend monitoring all of your healthcare and financial accounts for any suspicious activity or requesting that your bank or other credit card issuers issue you new credit cards. The Federal Trade Commission suggests the following steps if you believe your identity has been stolen or may be stolen:

1. Place a fraud alert on your credit reports and review your credit reports. Contact the toll-free fraud number of any of the three consumer reporting companies below to place a fraud alert on your credit report. **You only need to contact one of the three companies to place an alert.** The company you call is required to contact the other two companies.

    - ***Equifax***. 1-800-525-6285 – P.O. Box 740241, Atlanta, GA 30374-0241 – www.equifax.com;
    - ***Experian***. 1-888-EXPERIAN or 1-888-397-3742 – P.O. Box 9532, Allen, TX 75013 – www.experian.com;
    - ***TransUnion***. 1-800-680-7289 – Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790 – www.transunion.com.

Once you place the fraud alert, you are entitled to order free copies of your credit reports.

2. Carefully review your credit reports. Look for inquiries from companies that you haven't contacted, accounts that you did not open, and debts on your accounts that you can't explain. Be aware that some companies may bill under names other than their store names.
3. Close any accounts that you know, or believe, have been tampered with or opened fraudulently.
4. File your concern(s) with the Federal Trade Commission. This important information helps law enforcement agencies track down identity thieves. You can contact the Federal Trade Commission by calling 1-877-ID-THEFT (1-877-438-4338), or by visiting the Federal Trade Commission website at www.ftc.gov/idtheft, or by writing to the FTC at: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.
5. File a report with your local police or the police in the community where the identity theft took place. Further, you are entitled to request a copy of the police report filed in this matter.

Even if you do not find any signs of fraud on your credit reports, experts in identity theft recommend you check your credit reports every three months for the next year. We recommend that you carefully review your account statements, monitor your credit reports and report to law enforcement any instances of actual or suspected identity theft.

Other Important Information

Finally, you can request that a security freeze be placed on your credit file by contacting each of the three reporting agencies listed above and/or contacting the Federal Trade Commission to receive additional information regarding security freezes. Placing a freeze on your credit report 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 you wish to apply for any type of credit. Please note, because of more stringent security features, **you will need to place a security freeze separately with each of the three major credit reporting companies if you want the freeze on all of your credit files**. A security freeze remains on your credit file until you remove it or choose to lift it temporarily when applying for credit or credit-dependent services. When requesting a security freeze, be prepared to provide your name, address, social security number, and date of birth.

For More Information

If you have any questions or need any help with anything mentioned in this letter, please contact our information line by toll-free phone at 866-926-9801 or send an e-mail to databreach@airwayoxygeninc.com. In addition, if you believe that your information has been used without your authorization, please notify your local law enforcement officials immediately to enable them to promptly investigate the matter.

We take the security of those with whom we work and their data very seriously and our team is working diligently to ensure breaches of this type do not happen in the future.

Sincerely,

Stephen Nyhuis, President
Airway Oxygen Inc.

11852305/3

AIRWAY OXYGEN INC.
PO Box 9410
Wyoming, MI 49509

June [ ], 2017

[FName] [LName]
[Address1]
[Address 2]
[City], [State] [Zip]

Re: Notice of Data Breach

Dear [FName]:

We are sending this letter to you to inform you of a recent incident involving your personal information.

WHAT HAPPENED?

On the evening of April 18, 2017, we learned that unidentified criminal(s) had gained access to our technical infrastructure and installed ransomware in order to deny Airway Oxygen Inc. access to its own data. Ransomware is a type of malware that attempts to deny access to a user's data by encrypting data. Our records indicate that your protected health information was on the computer network. We have no indication that any of your protected health information stored on the computer network was accessed and acquired. Nevertheless, we wanted to provide notice to you so that you would be aware of the situation.

We truly regret that this incident has occurred and apologize for any difficulty or inconvenience it may cause you.

WHAT INFORMATION WAS INVOLVED?

The types of protected health information that were involved in the breach include some or all of the following data regarding our customer/end users and payment sources: full name, home address, birth date, social security number, telephone number, diagnosis, the type of service we are providing you, and health insurance policy numbers. No bank account numbers or debit or credit card numbers were exposed in the breach.

WHAT WE ARE DOING

Since learning of the incident, we immediately took steps to secure our internal systems against further intrusion, including by scanning the entire internal system, changing passwords for users, vendor accounts and applications, conducting a firewall review, updating and deploying security tools, and installing software to monitor and issue alerts as to suspicious firewall log activity. We have reported the incident to the FBI and will cooperate with their efforts. We have hired a cyber-security firm to assist in

conducting an investigation to assess the cause and impact of the breach. In addition, we are identifying further actions to reduce the risk of this situation recurring.

WHAT YOU CAN DO

We are keenly aware of how important your protected health information is to you.

As a security precaution, we recommend monitoring all of your healthcare and financial accounts for any suspicious activity or requesting that your bank or other credit card issuers issue you new credit cards. The Federal Trade Commission suggests the following steps if you believe your identity has been stolen or may be stolen:

1. Place a fraud alert on your credit reports and review your credit reports. Contact the toll-free fraud number of any of the three consumer reporting companies below to place a fraud alert on your credit report. **You only need to contact one of the three companies to place an alert.** The company you call is required to contact the other two companies.

   - ***Equifax***. 1-800-525-6285 – P.O. Box 740241, Atlanta, GA 30374-0241 – www.equifax.com;
   - ***Experian***. 1-888-EXPERIAN or 1-888-397-3742 – P.O. Box 9532, Allen, TX 75013 – www.experian.com;
   - ***TransUnion***. 1-800-680-7289 – Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790 – www.transunion.com.

Once you place the fraud alert, you are entitled to order free copies of your credit reports.

2. Carefully review your credit reports. Look for inquiries from companies that you haven't contacted, accounts that you did not open, and debts on your accounts that you can't explain. Be aware that some companies may bill under names other than their store names.
3. Close any accounts that you know, or believe, have been tampered with or opened fraudulently.
4. File your concern(s) with the Federal Trade Commission. This important information helps law enforcement agencies track down identity thieves. You can contact the Federal Trade Commission by calling 1-877-ID-THEFT (1-877-438-4338), or by visiting the Federal Trade Commission website at www.ftc.gov/idtheft, or by writing to the FTC at: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.
5. File a report with your local police or the police in the community where the identity theft took place. Further, you are entitled to request a copy of the police report filed in this matter.

Even if you do not find any signs of fraud on your credit reports, experts in identity theft recommend you check your credit reports every three months for the next year. We recommend that you carefully review your account statements, monitor your credit reports and report to law enforcement any instances of actual or suspected identity theft.

Other Important Information

Finally, you can request that a security freeze be placed on your credit file by contacting each of the three reporting agencies listed above and/or contacting the Federal Trade Commission to receive additional information regarding security freezes. Placing a freeze on your credit report 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 you wish to apply for any type of credit. Please note, because of more stringent security features, **you will need to place a security freeze separately with each of the three major credit reporting companies if you want the freeze on all of your credit files**. A security freeze remains on your credit file until you remove it or choose to lift it temporarily when applying for credit or credit-dependent services. When requesting a security freeze, be prepared to provide your name, address, social security number, and date of birth.

For More Information

If you have any questions or need any help with anything mentioned in this letter, please contact our information line by toll-free phone at 866-926-9801 or send an e-mail to databreach@airwayoxygeninc.com. In addition, if you believe that your information has been used without your authorization, please notify your local law enforcement officials immediately to enable them to promptly investigate the matter.

We take the security of those with whom we work and their data very seriously and our team is working diligently to ensure breaches of this type do not happen in the future.

Sincerely,

Stephen Nyhuis, President
Airway Oxygen Inc.

11852305/3