<<Date>> (Format: Month Day, Year)

<<MemberFirstName>> <<MemberMiddleName>> <<MemberLastName>> <<Suffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<ZipCode>>

RE: Notice of Data Privacy Incident

Dear <<MemberFirstName>> <<MemberLastName>>,

Reliable Respiratory ("Reliable") writes to make you aware of a recent incident that may affect the privacy of some of your personal information. While there is currently no evidence that your information has been misused, we are making you aware of the event, the steps we are taking in response, and steps you may take to better protect against possible misuse of your personal information, should you feel it appropriate to do so.

What Happened? On or around July 3, 2018, Reliable Respiratory ("Reliable") became aware of unusual activity in an employee's email account. Reliable took steps to investigate the unusual activity and determined that it had been the target of an email phishing campaign that resulted in the compromise of a Reliable employee's email credentials. Reliable immediately commenced an investigation, which included working with third party forensic specialists, to determine the full nature and scope of the incident. Through the investigation, Reliable determined that, as a result of the phishing event, an unauthorized actor(s) gained access to the employee email account between June 28 and July 2, 2018. The investigation also determined that the emails affected by this incident contained certain personal information.

What Information Was Involved? Through the investigation, Reliable determined that the information present in the impacted emails includes your: <<ClientDef1(DATA ELEMENTS)>>. While these elements were confirmed to be contained in the affected email account, we are not currently aware of any actual or attempted misuse of personal information potentially affected by this incident.

What We Are Doing. Reliable takes the confidentiality, privacy, and security of information in its care very seriously. Upon learning of unusual activity related to an employee's email account, Reliable immediately commenced an investigation to confirm the nature and scope of the incident and identify any individuals whose information may have been present in the emails potentially subject to unauthorized access. Reliable is taking steps to notify you of this event and provide you with information and access to resources you may use to better protect against potential misuse of personal information, should you feel it appropriate to do so. While Reliable has security measures in place to protect information in its care, we are also taking steps to implement additional safeguards and review policies and procedures in order to protect the security of information on our systems.

As an added precaution, Reliable is providing you with access to 12 months of credit monitoring and identity protection services from Kroll at no cost to you. A description of services and instructions on how to enroll can be found within the enclosed *Steps You Can Take to Protect Personal Information*. Please note that you must complete the enrollment process yourself, as we are not permitted to enroll you in these services on your behalf.

What You Can Do. You can review the enclosed *Steps You Can Take to Protect Personal Information*. You can also enroll to receive the free credit monitoring services and identity protection services through Kroll.

For More Information. We understand you may have questions about this incident that are not addressed in this letter. If you have questions or concerns, please call our dedicated hotline at 1-833-228-5714, Monday through Friday, 9am-6pm EST, excluding national holidays.

Please know Reliable takes the privacy and security of the personal information in our care very seriously and we sincerely regret any inconvenience or concern this incident may cause you.

Sincerely,

Reliable Respiratory

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services[1] from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

[1] Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Credit Monitoring

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **<<IDMonitoringURL>>** to activate and take advantage of your identity monitoring services.

*You have until **January 14, 2019** to activate your identity monitoring services.*

Membership Number: **<<Member ID>>**

To receive credit services by mail instead of online, please call 1-833-228-5714. Additional information describing your services is included with this letter.

Monitor Your Accounts

In addition to enrolling in the complimentary services detailed above, we encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements and explanation of benefits, and to monitor your credit reports for suspicious activity and to detect errors. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian
P.O. Box 9554
Allen TX 75013
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion
P.O. Box 2000
Chester, PA 19016
1-800-909-8872
www.transunion.com/credit-freeze

Equifax
PO Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian
P.O. Box 2002
Allen, TX 75013
1-888-397-3742
www.experian.com/fraud/center.html

TransUnion
P.O. Box 2000
Chester, PA 19106
1-800-680-7289
www.transunion.com/fraud-victim-resource/place-fraud-alert

Equifax
P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008
www.equifax.com/personal/credit-report-services

Additional Information

Although we have no reason to believe that your personal information has been used to file fraudulent tax returns, you can contact the IRS at www.irs.gov/Individuals/Identity-Protection for helpful information and guidance on steps you can take to address a fraudulent tax return filed in your name and what to do if you become the victim of such fraud. You can also visit www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft for more information.

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement. This notice has not been delayed by law enforcement.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, www.ncdoj.gov.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For Rhode Island Residents: The Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, 1-401-247-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are XXX Rhode Island residents impacted by this incident.

<<Date>> (Format: Month Day, Year)

Parent or Guardian of
<<MemberFirstName>> <<MemberMiddleName>> <<MemberLastName>> <<Suffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<ZipCode>>

RE: Notice of Data Privacy Incident

Dear Parent or Guardian of <<MemberFirstName>> <<MemberLastName>>,

Reliable Respiratory ("Reliable") writes to make you aware of a recent incident that may affect the privacy of some of your minor's personal information. While there is currently no evidence that your minor's information has been misused, we are making you aware of the event, the steps we are taking in response, and steps you may take to better protect against possible misuse of your minor's personal information, should you feel it appropriate to do so.

What Happened? On or around July 3, 2018, Reliable Respiratory ("Reliable") became aware of unusual activity in an employee's email account. Reliable took steps to investigate the unusual activity and determined that it had been the target of an email phishing campaign that resulted in the compromise of a Reliable employee's email credentials. Reliable immediately commenced an investigation, which included working with third party forensic specialists, to determine the full nature and scope of the incident. Through the investigation, Reliable determined that, as a result of the phishing event, an unauthorized actor(s) gained access to the employee email account between June 28 and July 2, 2018. The investigation also determined that the emails affected by this incident contained certain personal information.

What Information Was Involved? Through the investigation, Reliable determined that the information present in the impacted emails includes your minor's: <<ClientDef1(DATA ELEMENTS)>>. While these elements were confirmed to be contained in the affected email account, we are not currently aware of any actual or attempted misuse of personal information potentially affected by this incident.

What We Are Doing. Reliable takes the confidentiality, privacy, and security of information in its care very seriously. Upon learning of unusual activity related to an employee's email account, Reliable immediately commenced an investigation to confirm the nature and scope of the incident and identify any individuals whose information may have been present in the emails potentially subject to unauthorized access. Reliable is taking steps to notify you of this event and provide you with information and access to resources you may use to better protect your minor against potential misuse of personal information, should you feel it appropriate to do so. While Reliable has security measures in place to protect information in its care, we are also taking steps to implement additional safeguards and review policies and procedures in order to protect the security of information on our systems.

As an added precaution, Reliable is providing you with access to 12 months of minor monitoring and identity protection services from Kroll at no cost to you. A description of services and instructions on how to enroll can be found within the enclosed *Steps You Can Take to Protect Personal Information*. Please note that you must complete the enrollment process yourself, as we are not permitted to enroll your minor in these services on your behalf.

What You Can Do. You can review the enclosed *Steps You Can Take to Protect Personal Information*. You can also enroll your minor to receive the free minor monitoring services and identity protection services through Kroll.

For More Information. We understand you may have questions about this incident that are not addressed in this letter. If you have questions or concerns, please call our dedicated hotline at 1-833-228-5714, Monday through Friday, 9am-6pm EST, excluding national holidays.

Please know Reliable takes the privacy and security of the personal information in our care very seriously and we sincerely regret any inconvenience or concern this incident may cause you.

Sincerely,

Reliable Respiratory

TAKE ADVANTAGE OF MINOR IDENTITY MONITORING SERVICES

You've been provided with access to the following services[1] from Kroll:

Minor Identity Monitoring

Minor Identity Monitoring detects when names, addresses, and credit information is associated with your child's Social Security number. An alert will be sent when activity is detected. The presence of a credit file may be an indicator of identity theft or fraud for children who, as minors, should not have a credit history.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your minor's identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If your minor becomes a victim of identity theft, an experienced Kroll licensed investigator will work on their behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and will do most of the work for you. Your minor's investigator can dig deep to uncover all aspects of the identity theft, and then work to resolve it.

[1] Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari.

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Minor Monitoring

Visit **<<IDMonitoringURL>>** to activate and take advantage of Minor Identity Monitoring.

*You have until **January 14, 2019** to activate monitoring services for your child.*

Your Membership Number is: **<<Member ID>>**

After you have logged in for the first time, you will see a screen with the title "Confirm Your Information". Before Minor Identity Monitoring services can be activated, you must follow the instructions below:

1. Change the "First Name" and "Last Name" fields to a parent or guardian's name.
2. Change the address that appears to the parent or guardian's current address.
3. Enter the parent or guardian's date of birth and Social Security number.
4. Enter the email address and password you would like to use for the account. Choose a security question and enter the security answer.
5. Click the "Create Account" button. After the account is created, you will be able to activate your child's Identity monitoring service.

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your minor's account statements and explanation of benefits, and to monitor your minor's credit reports for suspicious activity and to detect errors.

While minors under the age of 18 typically do not have credit files, the following information relates to protecting one's credit once established:

Under U.S. law, adults are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of a credit report.

Adults have the right to place a "security freeze" on their credit report, which will prohibit a consumer reporting agency from releasing information in the consumer's credit report without the consumer's express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in an individual's name without consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in a credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application an individual makes regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, an individual cannot be charged to place or lift a security freeze on his or her credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian
P.O. Box 9554
Allen TX 75013
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion
P.O. Box 2000
Chester, PA 19016
1-800-909-8872
www.transunion.com/credit-freeze

Equifax
PO Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:Your full name (including middle initial as well as Jr., Sr., II, III, etc.);

1. Social Security number;
2. Date of birth;
3. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
4. Proof of current address, such as a current utility bill or telephone bill;
5. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
6. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, adults have the right to place an initial or extended "fraud alert" on a file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian
P.O. Box 2002
Allen, TX 75013
1-888-397-3742
www.experian.com/fraud/center.html

TransUnion
P.O. Box 2000
Chester, PA 19106
1-800-680-7289
www.transunion.com/fraud-victim-resource/place-fraud-alert

Equifax
P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008
www.equifax.com/personal/credit-report-services

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement. This notice has not been delayed by law enforcement.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, www.ncdoj.gov.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For Rhode Island Residents: The Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, 1-401-247-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are XXX Rhode Island residents impacted by this incident.