



MULLEN
COUGHLIN_{LLC}
ATTORNEYS AT LAW

M. Alexandra Bradley
Office: 267-930-4773
Fax: 267-930-4771
Email: abradley@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

July 20, 2018

INTENDED FOR ADDRESSEE(S) ONLY

VIA U.S. MAIL

Attorney General Gordon J. MacDonald
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Security Incident

Dear Attorney General MacDonald:

We represent NorthStar Anesthesia (“NorthStar”), 6225 State Highway 161, #200, Irving, TX 75038, and write to notify your office of an incident that may affect the security of some personal information relating to approximately twenty-eight (28) New Hampshire residents. By providing this notice, NorthStar does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

Between May 23 and 24, 2018, NorthStar learned of an email phishing campaign that resulted in the compromise of certain employees’ email credentials. NorthStar immediately took steps to respond and commenced an investigation to determine the nature and scope of the incident, as well as determine what information may be affected. The investigation included working with third party forensic investigators. Through the investigation, NorthStar determined that an unauthorized actor(s) gained access to certain employee email accounts between April 3 and May 24, 2018. The investigation also determined that the emails affected by this incident contained certain personal information.

The investigation determined that the following information related to New Hampshire residents was present in the email account at the time of the incident: name, health information, health insurance policy or subscriber number, and patient identification information.

Notice to New Hampshire Residents

On or about July 20, 2018, NorthStar will begin providing written notice of this incident to potentially affected individuals, which includes approximately twenty-eight (28) New Hampshire residents. Written notice is being provided in substantially the same form as the letter attached hereto as *Exhibit A*. On July 20, 2018, NorthStar will also be posting notice of this incident on the homepage of their website. This notice will appear in substantially the same form as the notice attached hereto as *Exhibit B*.

Other Steps Taken and To Be Taken

The confidentiality, privacy, and security of information in its care is one of NorthStar's highest priorities. Upon discovering the event, NorthStar immediately took steps to investigate and respond to the incident, including changing the affected users' email credentials. NorthStar has been working diligently, with the assistance of third party forensic investigators, to ensure the security of its email environment, determine the full nature and scope of the event, and identify potentially affected individuals. While NorthStar has measures in place to protect information in its systems, it is working to implement additional safeguards to protect the security of information.

NorthStar is providing potentially impacted individual with notice of this event. This notice includes an offer of access to credit monitoring and identity theft protection services for two (2) years through ID Experts. NorthStar is also providing potentially impacted individuals with guidance on how to better protect against identity theft and fraud, including information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and explanation of benefits form and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. NorthStar will also be providing notice of this event to other state regulators, as required by law, as well as the U.S. Department of Health and Human Services.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4773.

Very truly yours,



M. Alexandra Bradley of
MULLEN COUGHLIN LLC

MAB/ajd
Enclosure

EXHIBIT A



C/O ID Experts
P.O. Box 10444
Dublin, OH 43017-4044

[Individual Name]
[Address]
[City], [State] [Zip Code]

To Enroll, Please Call:
(888) 685-7768
Or Visit:
<https://ide.myidcare.com/northstar>
Enrollment Code: [XXXXXXXXXX]

July 20, 2018

RE: Notice of Data Privacy Event

Dear [Name]:

NorthStar Anesthesia, (“NorthStar”) writes to inform you of a recent event that may affect the privacy of some of your personal information. While, we have no evidence to date that your information has been misused, we are making you aware of this incident so you may take steps to better protect against possible misuse of your information, should you feel it appropriate to do so.

What Happened? Between May 23 and 24, 2018, NorthStar learned of an email phishing campaign that resulted in the compromise of certain employees’ email credentials. NorthStar immediately took steps to respond and commenced an investigation to determine the nature and scope of the incident, as well as determine what information may be affected. The investigation included working with third party forensic investigators. Through the investigation, NorthStar determined that an unauthorized actor(s) gained access to certain employee email accounts between April 3 and May 24, 2018. The investigation also determined that the emails affected by this incident contained your personal information.

What Information Was Involved? Our investigation determined that the following information related to you was present in the email account at the time of the incident: name{data elements}.

What We Are Doing. The confidentiality, privacy, and security of information in our care is one of our highest priorities. Upon learning the email phishing event, we commenced an investigation to confirm the nature and scope of the incident and identify any individuals who may be affected. We have been working, with the assistance of third party forensic investigators, to identify and notify potentially impacted individuals. While we have security measures in place to protect information in our care, we are also implementing additional safeguards to protect the security of information. We will also be reporting this incident to the U.S. Department of Health and Human Services and state regulators, as required by law.


As an added precaution, we are offering you access to two (2) years of credit monitoring and identity theft restoration service through ID Experts at no cost to you. A description of this product is provided in the attached materials, which also contain instructions about how to enroll (including your personal activation code). Please note that you must complete the enrollment process, as we are not able to enroll you in these services on your behalf.

What You Can Do. You may review the enclosed “Steps You Can Take To Protect Personal Information.” You may also enroll to receive the free identity theft protection and identity restoration services described above.

For More Information. We understand you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at (888) 685-7768 (toll free), 5 am - 5 pm Pacific Time, Monday through Friday.

Again, NorthStar takes the privacy and security of the personal information in our care seriously. We sincerely regret any inconvenience or concern this incident has caused you.

Sincerely,

A handwritten signature in black ink that reads "Sandra Geary". The signature is written in a cursive style with a large, looping 'S' and a long, sweeping tail on the 'y'.

Sandra Geary
Compliance Officer
NorthStar Anesthesia

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Credit Monitoring

While, to date, we have no evidence of actual or attempted misuse of any of the information potentially impacted by this incident, we encourage you to contact ID Experts to enroll in the two (2) years of MyIDCare services we are offering at no cost to you. MyIDCare representatives can answer questions or concerns you may have regarding protection of your personal information. Information on these services and how to enroll can be found below:

1. *To enroll online*, go to <https://ide.myidcare.com/northstar> and follow the instructions for enrollment using the Enrollment Code listed above.

2. *Activate the credit monitoring* provided as part of your MyIDCare membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, MyIDCare will be able to assist you.

3. *To enroll by phone*, contact MyIDCare at (888) 685-7768 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

MyIDCare experts are available Monday through Friday from 5 am - 5 pm Pacific Time. Please note the deadline to enroll is October 20, 2018.

Monitor Your Accounts

Credit Reports. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your personal account statements and explanation of benefit forms and monitoring your free 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. Contact information for the credit reporting agencies can be found below.

Fraud Alerts. At no charge, you can also have the three major credit bureaus place a “fraud alert” on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below:

Equifax
P.O. Box 105069
Atlanta, GA 30348
800-525-6285
www.equifax.com

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

TransUnion
P.O. Box 2000
Chester, PA 19106
800-680-7289
www.transunion.com

Security Freeze. You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer’s credit report without the consumer’s written authorization. However, please be advised 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. If you have been a victim of identity theft, and you provide the credit bureau with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. Fees vary based on where you live, but commonly range from \$3 to \$15. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files. In order to request a security freeze, you will need to supply your full name, address, date of birth, Social Security number, current address, all addresses for up to five previous years, email address, a copy of your state identification card or driver’s license, and a copy of a utility bill, bank or insurance statement, or other statement proving residence. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
1-800-685-1111
www.freeze.equifax.com

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/

TransUnion
P.O. Box 2000
Chester, PA 19016
1-888-909-8872
freeze.transunion.com

Additional Information. You can further educate yourself regarding identity theft, security freezes, fraud alerts, and the steps you can take to protect yourself against identity theft and fraud by contacting the Federal Trade Commission or your state Attorney General, as well as the credit reporting agencies listed above. 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); and TTY: 1-866-653-4261. The Federal Trade Commission encourages those who discover that their information has been misused to file a complaint with them. Instances of known or suspected identity theft should be reported to law enforcement, the Federal Trade Commission, and your state Attorney General. This notice has not been delayed as the result of a law enforcement investigation.

For Maryland residents, the Maryland Attorney General can be reached at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and www.oag.state.md.us. NorthStar Anesthesia is located at 6225 State Highway 161, Suite 200.

For North Carolina residents, the North Carolina Attorney General can be contacted by mail at 9001 Mail Service Center, Raleigh, NC 27699-9001; by phone toll-free at 1-877-566-7226; by phone at 1-919-716-6400; and online at www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General can be contacted by mail at 150 South Main Street, Providence, RI 02903; by phone at (401) 274-4400; and online at www.riag.ri.gov. A total of {NUMBER} Rhode Island residents are potentially impacted by this incident. You have the right to file and obtain a police report if you ever experience identity theft or fraud. Please note that, in order to file a crime report or incident report with law enforcement for identity theft, you may be asked to provide some kind of proof that you have been a victim.

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 a 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 to the Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

EXHIBIT B

NOTICE OF DATA PRIVACY EVENT

ABOUT THE DATA PRIVACY EVENT

NorthStar Anesthesia, (“NorthStar”) recently discovered an event that may affect the security of some personal information in NorthStar’s care. We are providing notice of the event so potentially affected individuals may take steps to better protect against possible misuse of information, should they feel it appropriate to do so.

FREQUENTLY ASKED QUESTIONS

Q. What Happened? Between May 23 and 24, 2018, NorthStar learned of an email phishing campaign that resulted in the compromise of certain employees’ email credentials. NorthStar immediately took steps to respond and commenced an investigation to determine the nature and scope of the incident, as well as determine what information may be affected. The investigation included working with third party forensic investigators. Through the investigation, NorthStar determined that an unauthorized actor(s) gained access to certain employee email accounts between April 3 and May 24, 2018. The investigation also determined that the emails affected by this incident contained personal information.

Q. What Information Was Involved? While the information potentially affected varies by individual, NorthStar’s investigation determined that the information that may have been affected includes name, date of birth, health insurance application or claims information, health insurance policy or subscriber number, health information, IRS identity protection number, taxpayer identification number, medical history information, treatment and diagnosis information, and medical record number. For certain individuals, this incident may have also affected Social Security number.

Q. What is NorthStar Doing to respond? The confidentiality, privacy, and security of information in our care is one of our highest priorities. Upon learning of the email phishing event, we commenced an investigation to confirm the nature and scope of the incident and identify any individuals who may be affected. We have been working, with the assistance of third party forensic investigators, to identify and notify potentially impacted individuals. NorthStar is also offering potentially impacted individuals access to credit monitoring and identity restoration services for two (2) years at no cost.

While we have security measures in place to protect information in our care, we are also implementing additional safeguards to protect the security of information. NorthStar has also provided notice of this incident to the U.S. Department of Health and Human Services, as well as required state regulators.

Q. What Can I Do to Protect My Information?

Monitor Your Accounts

Credit Reports. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your personal account statements and explanation of benefit forms and monitoring your free 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. Contact information for the credit reporting agencies can be found below.

Fraud Alerts. At no charge, you can also have the three major credit bureaus place a “fraud alert” on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name.

Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below:

Equifax
P.O. Box 105069
Atlanta, GA 30348
800-525-6285
www.equifax.com

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

TransUnion
P.O. Box 2000
Chester, PA 19106
800-680-7289
www.transunion.com

Security Freeze. You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised 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. If you have been a victim of identity theft, and you provide the credit bureau with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. Fees vary based on where you live, but commonly range from \$3 to \$15. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files. In order to request a security freeze, you will need to supply your full name, address, date of birth, Social Security number, current address, all addresses for up to five previous years, email address, a copy of your state identification card or driver's license, and a copy of a utility bill, bank or insurance statement, or other statement proving residence. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
1-800-685-1111
www.freeze.equifax.com

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/

TransUnion
P.O. Box 2000
Chester, PA 19016
1-888-909-8872
freeze.transunion.com

Additional Information

You can further educate yourself regarding identity theft, security freezes, fraud alerts, and the steps you can take to protect yourself against identity theft and fraud by contacting the Federal Trade Commission or your state Attorney General, as well as the credit reporting agencies listed above. 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); and TTY: 1-866-653-4261. The Federal Trade Commission encourages those who discover that their information has been misused to file a complaint with them. Instances of known or suspected identity theft should be reported to law enforcement, the Federal Trade Commission, and your state Attorney General. Notice of this incident was not delayed as the result of a law enforcement investigation.

For Maryland residents, the Maryland Attorney General can be reached at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and www.oag.state.md.us. NorthStar Anesthesia is located at 6225 State Highway 161, Suite 200.

For North Carolina residents, the North Carolina Attorney General can be contacted by mail at 9001 Mail Service Center, Raleigh, NC 27699-9001; by phone toll-free at 1-877-566-7226; by phone at 1-919-716-6400; and online at www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General can be contacted by mail at 150 South Main Street, Providence, RI 02903; by phone at (401) 274-4400; and online at www.riag.ri.gov. To date, approximately 20 Rhode Island residents are known to be potentially impacted by this incident. You have the right to file and obtain a police report if you ever experience identity theft or fraud. Please note that, in order to file a crime report or incident report with law enforcement for identity theft, you may be asked to provide some kind of proof that you have been a victim.

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 a 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 to the Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For Massachusetts residents, you have the right to file and obtain a police report if you ever experience identity theft or fraud. Please note that, in order to file a crime report or incident report with law enforcement for identity theft, you may be asked to provide some kind of proof that you have been a victim. If you have been the victim of identity theft, and you provide a credit reporting agency with a valid police report, it cannot charge you to place, lift or remove a security freeze. In all other cases, a credit reporting agency may charge up to \$5 to place, temporarily lift, or permanently remove a security freeze. The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit file report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both, that can be used by you to authorize the removal or lifting of the security freeze. To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and Social Security number) **and** the PIN number or password provided to you when you placed the security freeze, as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and Social Security number) **and** the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

Q. Where Can I Go To Get More Information? NorthStar has set up a dedicated assistance line to answer questions regarding this incident. The dedicated assistance line may be reached at (888) 685-7768 (toll free), Monday through Friday from 7 am - 7 pm Central Time.