



MULLEN  
COUGHLIN...

STATE OF NH  
DEPT OF JUSTICE

2017 APR 28 AM 11:55

Sian M. Schafle  
Office: 267-930-4799  
Fax: 267-930-4771  
Email: [sschafle@mullen.law](mailto:sschafle@mullen.law)

1275 Drummers Lane, Suite 302  
Wayne, PA 19087

April 21, 2017

**VIA U.S. MAIL**

Attorney General Joseph Foster  
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 Foster:

We represent Atlantic Digestive Specialists ("ADS"), 21 Clark Way, Route 108, Somersworth, NH 03878, and are writing to notify your office of an incident that may affect the security of personal information relating to 1,505 New Hampshire residents. The investigation into this event is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, ADS does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

**Nature of the Data Event**

On February 20, 2017, ADS discovered that some of its systems were infected with ransomware. ADS removed the ransomware from the affected systems by February 22, 2017. ADS has been working diligently, with the assistance of third-party forensic investigators, to determine the full nature and scope of this incident. To date, the investigation has determined the ransomware began affecting the systems on or around February 18, 2017.

While the investigation is ongoing, to date, ADS has no evidence of any actual or attempted misuse of information as a result of this incident. However, the systems that were impacted by this incident may have contained information including name, date of birth, address information, telephone number, medical record number, health insurance information, and clinical/diagnostic information. For some individuals, the impacted information may have also included a Social Security number.

### **Notice to New Hampshire Residents**

On April 21, 2017, ADS will begin providing written notice of this incident to those individuals the investigation has determined had information stored on the affected system, which includes 1,505 New Hampshire residents. Written notice will be provided in substantially the same form as the letter attached here as *Exhibit A*. ADS also published notice of this event on their website beginning on April 21, 2017. This posting is attached hereto as *Exhibit B*. Additionally, on April 21, 2017, ADS provided notice to statewide media in New Hampshire. This notice is attached hereto as *Exhibit C*.

### **Other Steps Taken and To Be Taken**

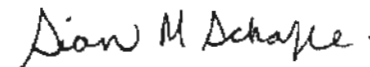
Upon discovering the fraudulent nature of the email, ADS moved quickly to identify the individuals who may be affected, to put in place resources to assist them, and to provide them with notice of this incident.

ADS is providing all potentially affected individuals access to 12 months of credit and identity monitoring services, including identity restoration services, through Equifax, and has established a dedicated call center for potentially affected individuals to contact with questions or concerns regarding this incident. Additionally, ADS is 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, information on protecting against tax fraud, 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 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. ADS is also providing written notice of this incident to other state regulators as necessary. ADS has provided notice of this incident to the FBI.

### **Contact Information**

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at 267-930-4799.

Very truly yours,



Sian Schafle of  
MULLEN COUGHLIN LLC

# **EXHIBIT A**



# Atlantic Digestive SPECIALISTS

STATE OF NH  
DEPT OF JUSTICE

2017 APR 28 AM 11:56

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

April 21, 2017

## Re: Notice of Data Privacy Incident

Dear [Name]:

Atlantic Digestive Specialists (“ADS”) is writing to inform you of an incident that may affect the security of your personal health information. While ADS is unaware of any actual or attempted misuse of your information, this letter contains details about the incident and our response, as well as steps you can take to protect your personal information, should you feel it appropriate to do so.

**What Happened?** On February 20, 2017, ADS discovered that some of our systems were infected with ransomware. ADS removed the ransomware from the affected systems by February 22, 2017. We have been working diligently, with the assistance of third-party forensic investigators, to determine the full nature and scope of this incident. To date, the investigation has determined the ransomware began affecting the systems on or around February 18, 2017.

**What Information Was Involved?** While our investigation is ongoing, to date, we have no evidence of any actual or attempted misuse of your information as a result of this incident. However, the systems that were impacted by this incident may have contained information including your name, date of birth, address information, telephone number, medical record number, health insurance information, and clinical/diagnostic information. For some individuals, the impacted information may have also included a Social Security number.

**What We Are Doing.** The confidentiality, privacy, and security of our patient information is one of our highest priorities. We have stringent security measures in place to protect the security of information in our possession. In addition, as part of our ongoing commitment to the security of personal information in our care, we are working to implement additional safeguards and security measures to enhance the privacy and security of information on our systems. We have contacted the FBI and will be contacting the relevant state Attorneys General. We have also reported this incident to the U.S. Department of Health and Human Services (HHS).

As an added precaution, we have arranged to have Equifax protect your identity for 12 months at no cost to you. The cost of this service will be paid for by ADS. We encourage you to enroll in these services, as we are not able to act on your behalf to enroll you in the credit monitoring service. Instructions on how to enroll in the Equifax services can be found in the enclosed *Steps You Can Take to Protect Your Information*.

**What You Can Do.** You can enroll to receive the free credit monitoring and identity restoration services described above. You may also review the enclosed *Steps You Can Take to Protect Your Information* for

more information on the Equifax services and other information you can use to better protect against the misuse of your information, should you feel it appropriate to do so.

***For More Information.*** We understand that 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 888-757-1875 (toll free), Monday through Friday, 9:00 a.m. to 9:00 p.m. EDT.

We sincerely regret any inconvenience or concern this incident has caused you.

Sincerely,

A handwritten signature in cursive script, appearing to read "David Hutton".

David Hutton  
Practice Administrator  
Atlantic Digestive Specialists  
21 Clark Way, Route 108  
Somersworth, NH 03878



## Steps You Can Take to Protect Your Information

While we continue to investigate, you may take direct action to further protect against possible identity theft or financial loss.

**Credit Monitoring – provided by ADS.** We have partnered with Equifax® to provide its Credit Watch™ Gold identity theft protection product for one year at no cost to you.

*About the Product.* Equifax Credit Watch will provide you with an “early warning system” to changes to your credit file. Note: You must be over age 18 with a credit file in order to take advantage of the product. Equifax Credit Watch provides you with the following key features and benefits:

- Comprehensive credit file monitoring and automated alerts of key changes to your **Equifax** credit report
- Wireless alerts and customizable alerts available (available online only)
- Access to your Equifax Credit Report™
- Up to \$25,000 in identity theft insurance with \$0 deductible, at no additional cost to you\*
- Live agent Customer Service 7 days a week from 8 a.m. to 3 a.m. to assist you in understanding the content of your Equifax credit information, to provide personalized identity theft victim assistance, and help initiate an investigation of inaccurate information.
- 90-day Fraud Alert placement with automatic renewal functionality (available online only)†

*How to Enroll.* You can sign up online or over the phone.

To sign up online for online delivery go to [www.myservices.equifax.com/gold](http://www.myservices.equifax.com/gold) and follow the instructions below:

1. **Welcome Page:** Enter the Activation Code **CODE** in the “Activation Code” box and click the “Submit” button.
2. **Register:** Complete the form with your contact information (name, gender, home address, date of birth, Social Security Number and telephone number) and click the “Continue” button.
3. **Create Account:** Complete the form with your email address, create a User Name and Password, check the box to accept the Terms of Use and click the “Continue” button.
4. **Verify ID:** The system will then ask you up to four security questions to verify your identity. Please answer the questions and click the “Submit Order” button.
5. **Order Confirmation:** This page shows you your completed enrollment. Please click the “View My Product” button to access the product features.

To sign up by phone for US Mail delivery, dial 1-866-937-8432 for access to the Equifax Credit Watch automated enrollment process. Note that all credit reports and alerts will be sent to you via US Mail only.

1. **Activation Code:** You will be asked to enter your enrollment code as provided in Step 1 of the online enrollment instructions above.

---

\* Identity Theft Insurance underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions. This product is not intended for minors (under 18 years of age).

† The Automatic Fraud Alert feature made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.

2. **Customer Information:** You will be asked to enter your home telephone number, home address, name, date of birth and Social Security Number.
3. **Permissible Purpose:** You will be asked to provide Equifax with your permission to access your credit file and to monitor your file. Without your agreement, Equifax cannot process your enrollment.

**Order Confirmation:** Equifax will provide a confirmation number with an explanation that you will receive your Fulfillment Kit via the US Mail (when Equifax is able to verify your identity) or a Customer Care letter with further instructions (if your identity can not be verified using the information provided). Please allow up to 10 business days to receive this information.

*We encourage you* to enroll in the credit monitoring services we are offering, at no cost to you, as we are not able to act on your behalf to enroll you in the credit monitoring service.

**Contact the IRS.** You may contact the IRS at [www.irs.gov/Individuals/Identity-Protection](http://www.irs.gov/Individuals/Identity-Protection) for helpful information and guidance on steps you can take to prevent a fraudulent tax return from being 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](http://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft) for more information.

### **Monitor Your Accounts.**

**Credit Reports.** We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports and explanation of benefits forms for suspicious activity. 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](http://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.

**Fraud Alerts.** At no charge, you can also have these 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](http://www.equifax.com)

Experian  
P.O. Box 2002  
Allen, TX 75013  
888-397-3742  
[www.experian.com](http://www.experian.com)

TransUnion  
P.O. Box 2000  
Chester, PA 19106  
800-680-7289  
[www.transunion.com](http://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	Experian Security Freeze	TransUnion
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
1-800-685-1111	1-888-397-3742	1-888-909-8872
<a href="https://www.freeze.equifax.com">https://www.freeze.equifax.com</a>	<a href="http://www.experian.com/freeze/">www.experian.com/freeze/</a>	<a href="http://www.transunion.com/">www.transunion.com/</a>

**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.

*The Federal Trade Commission* can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; [www.identitytheft.gov](http://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.

*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](http://www.riag.ri.gov). To date, there is 1 Rhode Island resident that may be 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 will likely need to provide some kind of proof that you have been a victim.

*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 will likely need to provide some kind of proof that you have been a victim.

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.





# Atlantic Digestive SPECIALISTS

STATE OF NH  
DEPT OF JUSTICE  
2017 APR 20 AM 11:56

Parent/Guardian of  
Name  
Address  
City State Zip

April 21, 2017

## Re: Notice of Data Privacy Incident

Dear Parent/Guardian of [Recipient Name]:

Atlantic Digestive Specialists (“ADS”) is writing to inform you of an incident that may affect the security of your son or daughter’s personal health information. While ADS is unaware of any actual or attempted misuse of your son or daughter’s information, this letter contains details about the incident and our response, as well as steps you can take to protect your child’s information, should you feel it appropriate to do so.

**What Happened?** On February 20, 2017, ADS discovered that some of our systems were infected with ransomware. ADS removed the ransomware from the affected systems by February 22, 2017. We have been working diligently, with the assistance of third-party forensic investigators, to determine the full nature and scope of this incident. To date, the investigation has determined the ransomware began affecting the systems on or around February 18, 2017.

**What Information Was Involved?** While our investigation is ongoing, to date, we have no evidence of any actual or attempted misuse of your son or daughter’s information as a result of this incident. However, the systems that were impacted by this incident may have contained your son or daughter’s information including name, date of birth, address information, telephone number, medical record number, health insurance information, and clinical/diagnostic information. For some individuals, the impacted information may have also included a Social Security number.

**What We Are Doing.** The confidentiality, privacy, and security of our patient information is one of our highest priorities. We have stringent security measures in place to protect the security of information in our possession. In addition, as part of our ongoing commitment to the security of personal information in our care, we are working to implement additional safeguards and security measures to enhance the privacy and security of information on our systems. We have contacted the FBI and will be contacting the relevant state Attorneys General. We have also reported this incident to the U.S. Department of Health and Human Services (HHS).

As an added precaution, we have arranged to have Equifax protect your son or daughter’s identity for 12 months at no cost to you. The cost of this service will be paid for by ADS. We encourage you to enroll in these services as we are not able to act on your behalf to enroll your son or daughter in the

identity monitoring service. Instructions on how to enroll in the Equifax services can be found in the enclosed *Steps You Can Take to Protect Your Information*.

***What You Can Do.*** You can enroll your son or daughter to receive Equifax's monitoring product described above. You may also review the enclosed *Steps You Can Take to Protect Your Information* for more information on the Equifax services and other information you can use to better protect against the misuse of your son or daughter's information, should you feel it appropriate to do so.

***For More Information.*** We understand that 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 888-757-1875 (toll free), Monday through Friday, 9:00 a.m. to 9:00 p.m. EDT.

We sincerely regret any inconvenience or concern this incident has caused you.

Sincerely,

A handwritten signature in black ink, appearing to read "David Hutton". The signature is written in a cursive style with a large initial "D".

David Hutton  
Practice Administrator  
Atlantic Digestive Specialists  
21 Clark Way, Route 108  
Somersworth, NH 03878

## Steps You Can Take to Protect Your Information

While we continue to investigate, you may take direct action to further protect against possible identity theft or financial loss.

**Credit Monitoring – provided by ADS.** We have arranged to have Equifax Personal Solutions help you to protect your minor's personal information at no cost to you.

*About the Product.* Equifax Child Identity Monitoring will scan the Equifax credit database for any instances of the minor's social security number and look for a copy of the minor's credit file.

- If no SSN match is found and no credit file exists, Equifax will create a credit file in the minor's name and immediately "lock" the credit file. This will prevent access to the minor's information in the future. If someone attempts to use your minor's information to open credit, you will receive an email alert.
- If there is a match and a credit file exists, Equifax will immediately "lock" the file, initiate an investigation into the use of that file and alert you to new attempts to use your minor's information.

*How to Enroll.* Parents or guardians – if you have not ordered from Equifax in the past, you will need to create an account. If you have questions for Equifax, you may call the phone number listed in the Equifax Member Center or in the Equifax email communication.

To sign up your child please visit [www.myservices.equifax.com/minor](http://www.myservices.equifax.com/minor) and follow the steps below:

1. If you are a parent/guardian who already has an Equifax account, please login using the username and password you created when enrolling in your product.
2. If you are a parent/guardian who does not have an Equifax account, below the login screen, you will see text that reads "Don't have an Equifax account? Please click here to create an account." Please click to create your account, and then enter in the **parent/guardian** information on the screens that follow in order to create an account.
3. Select the button for "\$29.95 for 12 months".
4. Enter promotion code **CODE** to order the first minor product and click "apply code". This will zero out the price of the product. **Do not enter credit card information.**
5. Check the box to agree to the Terms of Use.
6. Next, click the "Continue" button.
7. You will be prompted to answer certain authentication questions to validate your identity.
8. Please review the order and click the "Submit" button.
9. You will then see the Order Confirmation. Please note that since you did not enter credit card information you **will not** be billed after the 12 months.
10. Click "View my Product" which will take you to your Member Center.
11. Click the orange button "Enroll Child" to enter your child's information (child's name, Date of Birth and Social Security Number). Note: if you enter the child's SSN incorrectly, you will need to remove the minor by going to your Member Center and clicking on "My Account" to



remove the minor from monitoring the account. You may then re-enroll the minor with the correct SSN.

12. Check the box confirming you are the child's parent or guardian.
13. Click "Submit" to enroll your child.
14. If you are enrolling multiple minors, please log out, then repeat the above process to add another minor.

*We encourage you* to enroll your son or daughter in Equifax's monitoring services we are offering, at no cost to you, as we are not able to act on your child's behalf to enroll him or her in the monitoring service.

**Contact the IRS.** You may contact the IRS at [www.irs.gov/Individuals/Identity-Protection](http://www.irs.gov/Individuals/Identity-Protection) for helpful information and guidance on steps you can take to prevent a fraudulent tax return from being filed in your son or daughter's name and what to do if he or she becomes the victim of such fraud. You can also visit [www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft](http://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft) for more information.

### **Monitor Your Accounts.**

*Credit Reports.* We encourage you to remain vigilant against incidents of identity theft and fraud, to review applicable account statements, and to monitor your child's credit reports (should they maintain credit files) and explanation of benefits forms for suspicious activity. 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](http://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.

*Fraud Alerts.* At no charge, you can also have these credit bureaus place a "fraud alert" on your son or daughter's file (should such credit file exist) that alerts creditors to take additional steps to verify identity prior to granting credit in your child's name. Note, however, that because it tells creditors to follow certain procedures to protect your child, it may also delay in the 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](http://www.equifax.com)

Experian  
P.O. Box 2002  
Allen, TX 75013  
888-397-3742  
[www.experian.com](http://www.experian.com)

TransUnion  
P.O. Box 2000  
Chester, PA 19106  
800-680-7289  
[www.transunion.com](http://www.transunion.com)

*Security Freeze.* You may also place a security freeze on your son or daughter's credit file (should such files exist). 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 a credit report may delay, interfere with, or prevent the



timely approval of any requests your child may make for new loans, credit mortgages, employment, housing, or other services. If your child has 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 child's credit files. In order to request a security freeze, you will need to supply your child's 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

<https://www.freeze.equifax.com>

Experian Security Freeze

P.O. Box 9554

Allen, TX 75013

1-888-397-3742

[www.experian.com/freeze/](http://www.experian.com/freeze/)

TransUnion

P.O. Box 2000

Chester, PA 19016

1-888-909-8872

[www.transunion.com/](http://www.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.

*The Federal Trade Commission* can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; [www.identitytheft.gov](http://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.

*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](http://www.riag.ri.gov). To date, there is 1 Rhode Island resident that may be 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 will likely need to provide some kind of proof that you have been a victim.

*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 will likely need to provide some kind of proof that you have been a victim.

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.



# Atlantic Digestive SPECIALISTS

STATE OF NH  
DEPT OF JUSTICE  
2017 APR 28 AM 11:56

To the Next of Kin of  
[Name]  
[Address]  
[City, State, Zip]

April 21, 2017

## Re: Notice of Data Privacy Incident

Dear Next of Kin of [Recipient Name]:

Atlantic Digestive Specialists (“ADS”) is writing to inform you of an incident that may affect the security of your loved one’s personal health information. While ADS is unaware of any actual or attempted misuse of this information, this letter contains details about the incident and our response, as well as steps you can take to protect your loved one’s information, should you feel it appropriate to do so.

**What Happened?** On February 20, 2017, ADS discovered that some of our systems were infected with ransomware. ADS removed the ransomware from the affected systems by February 22, 2017. We have been working diligently, with the assistance of third-party forensic investigators, to determine the full nature and scope of this incident. To date, the investigation has determined the ransomware began affecting the systems on or around February 18, 2017.

**What Information Was Involved?** While our investigation is ongoing, we have no evidence of actual or attempted misuse of your one’s information as a result of this incident. However, the systems that were impacted by this incident may have contained your loved one’s information including name, date of birth, address information, telephone number, medical record number, health insurance information, and clinical/diagnostic information. For some individuals, the impacted information may have also included a Social Security number.

**What We Are Doing.** The confidentiality, privacy, and security of our patient information is one of our highest priorities. We have stringent security measures in place to protect the security of information in our possession. In addition, as part of our ongoing commitment to the security of personal information in our care, we are working to implement additional safeguards and security measures to enhance the privacy and security of information on our systems. We have contacted the FBI and will be contacting the relevant state Attorneys General. We have also reported this incident to the U.S. Department of Health and Human Services (HHS).

**What You Can Do.** We encourage you to review the attached *Steps You Can Take to Protect Your Information*. ADS also encourages you to remain vigilant against the misuse of your loved one’s information. You can do this by reviewing your loved one’s account statements, medical bills, and health insurance Explanation of Benefits statements regularly for suspicious activity.

***For More Information.*** We understand that 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 888-757-1875 (toll free), Monday through Friday, 9:00 a.m. to 9:00 p.m. EDT.

We sincerely regret any inconvenience or concern this incident has caused you.

Sincerely,

A handwritten signature in cursive script, appearing to read "David Hutton".

David Hutton  
Practice Administrator  
Atlantic Digestive Specialists  
21 Clark Way, Route 108  
Somersworth, NH 03878



## Steps You Can Take to Protect Your Loved One's Information

While we continue to investigate, you may take direct action to further protect against possible identity theft or financial loss.

**Monitoring Accounts:** We encourage you to remain vigilant against incidents of identity theft and fraud, by reviewing account statements, medical bills, and health insurance statements regularly for suspicious activity, to ensure that no one has submitted fraudulent medical claims using your loved one's name and other information. Report all suspicious or fraudulent charges to your loved one's account and insurance providers. If your loved one did not receive regular Explanation of Benefits statements, you can contact your loved one's health plan and request them to send such statements following the provision of services.

In addition, there are steps you can take to protect your loved one's credit file. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus so long as you verify your authorization to make such a request on behalf of your loved one. To order this free credit report, visit [www.annualcreditreport.com](http://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 this credit report. We recommend contacting the three credit reporting agencies listed below to discuss your particular situation and obtain specific guidance. Once you establish a relationship with the credit reporting agency and verify your authorization to make a request on behalf of your loved one, you can request a copy of your loved one's credit report. A review of the credit report will let you know of any active credit accounts that still need to be closed or any pending collection notices. Be sure to ask for all contact information on accounts currently open in your loved one's name (credit granters, collection agencies, etc.) so that you can follow through with these entities.

You may also request, in writing, that the credit report list the following alert:

"Deceased. Do not issue credit. If an application is made for credit, notify the following person(s) immediately: (list yourself, and/or another authorized relative, and/or executor/trustee of the estate—noting the relationship of any individual listed to your family member—and/or a law enforcement agency)."

In most cases, this flag will prevent the opening of new credit accounts in your loved one's name. Contact information for the three major credit bureaus is as follows:

Equifax  
P.O. Box 105069  
Atlanta, GA 30348  
800-525-6285  
[www.equifax.com](http://www.equifax.com)

Experian  
P.O. Box 2002  
Allen, TX 75013  
888-397-3742  
[www.experian.com](http://www.experian.com)

TransUnion  
P.O. Box 2000  
Chester, PA 19022  
800-680-7289  
[www.transunion.com](http://www.transunion.com)

**Additional Information.** You can further educate yourself regarding identity theft, security freezes, fraud alerts, and the steps you can take to protect against identity theft and fraud by contacting 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](http://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.

**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](http://www.riag.ri.gov). To date, there is 1 Rhode Island resident that may be impacted by this incident. You have the right to file and obtain a police report if you learn your loved one has 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 will likely need to provide some kind of proof that your loved one has been a victim.

**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 will likely need to provide some kind of proof that you have been a victim.

# **EXHIBIT B**

## **NOTICE OF DATA PRIVACY EVENT**

### **ABOUT THE DATA PRIVACY EVENT**

On February 20, 2017, ADS discovered that some of our systems were infected with ransomware. Our investigation revealed that the ransomware began affecting these systems on or around February 18, 2017. We removed the ransomware from the affected systems by February 22, 2017. We have been working diligently, with the assistance of third-party forensic investigators, to determine the full nature and scope of this incident. As part of our investigation, we also notified the FBI.

We continue to work closely with our third-party forensic investigators to investigate this incident and to confirm the security of our systems. We are also taking additional actions to strengthen and enhance the security of our systems moving forward.

### **FREQUENTLY ASKED QUESTIONS**

**Q: What happened?** ADS has been the target of a sophisticated cyberattack that resulted in ransomware infecting certain IT systems. While our investigation is ongoing, we have no evidence of any actual or attempted misuse of information as a result of this incident. The confidentiality, privacy, and security of information within our care is one of our highest priorities and we are taking proactive steps to address this incident.

**Q: What information may have been affected by this incident?** Again, while our investigation is ongoing, to date, we have no evidence of any actual or attempted misuse of information as a result of this incident. However, the systems that were impacted by this incident may have contained information including names, dates of birth, address information, telephone numbers, medical record numbers, health insurance information, and clinical/diagnostic information at the time of the incident. In limited instances, the impacted systems may have also contained Social Security numbers.

**Q: How will I know if I am affected by this incident?** On April 21, 2017, ADS began mailing notice letters to individuals whose data was present on the affected systems. ADS will continue the notification process should additional individuals be determined to be potentially impacted. In the meantime, if you believe you may be impacted, you may call our dedicated assistance line at 888-757-1875 (toll free), Monday through Friday, 9:00 a.m. to 9:00 p.m. EDT.

**Q: Is ADS providing impacted individuals access to credit monitoring services?** Yes, ADS is providing potentially impacted individuals access to credit monitoring services. Information on these services is included in the notice letter mailed to individuals whose information was on the affected systems.

**Q: What may I do to protect my information?**

#### **Monitor Your Accounts.**

*Credit Reports.* We encourage impacted individuals to remain vigilant against incidents of identity theft and fraud, to review account statements, and to monitor their credit reports and



explanation of benefits forms for suspicious activity. 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](http://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.

*Fraud Alerts.* At no charge, you can also have these 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](http://www.equifax.com)

Experian  
P.O. Box 2002  
Allen, TX 75013  
888-397-3742  
[www.experian.com](http://www.experian.com)

TransUnion  
P.O. Box 2000  
Chester, PA 19106  
800-680-7289  
[www.transunion.com](http://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](http://www.freeze.equifax.com)

Experian Security Freeze  
P.O. Box 9554  
Allen, TX 75013  
1-888-397-3742  
[www.experian.com/freeze/](http://www.experian.com/freeze/)

TransUnion  
P.O. Box 2000  
Chester, PA 19016  
1-888-909-8872  
[www.transunion.com/](http://www.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.

*The Federal Trade Commission* can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; [www.identitytheft.gov](http://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.



*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](http://www.riag.ri.gov). 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 will likely need to provide some kind of proof that you have been a victim. To date, a total of 1 Rhode Island resident may be impacted by this incident.

*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 will likely need to provide some kind of proof that you have been a victim.

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.

# **EXHIBIT C**

*NOTICE TO MEDIA*

FOR IMMEDIATE RELEASE

RE: Atlantic Digestive Specialists, Notice of Data Breach

**Somersworth, NH (April 21, 2017)** – On February 20, 2017, Atlantic Digestive Specialists (“ADS”) discovered that some of its systems were infected with ransomware. ADS removed the ransomware from the affected systems by February 22, 2017. ADS has been working diligently, with the assistance of third-party forensic investigators, to determine the full nature and scope of this incident. To date, the investigation has determined the ransomware began affecting the systems on or around February 18, 2017.

While ADS’s investigation is ongoing, to date, ADS has no evidence of any actual or attempted misuse of information as a result of this incident. However, the systems that were impacted by this incident may have contained information including an individual’s name, date of birth, address information, telephone number, medical record number, health insurance information, and clinical/diagnostic information. For some individuals, the impacted information may have also included a Social Security number.

On April 21, 2017, ADS began mailing notice letters to potentially impacted individuals. ADS has offered potentially impacted individuals access to credit monitoring and identity theft protection services for one year without charge. ADS is encouraging potentially impacted individuals to remain vigilant against incidents of identity theft and fraud, to review account statements, and to monitor credit reports and explanation of benefits forms for suspicious activity. ADS’s notification to potentially impacted individuals includes information such as obtaining a free credit report annually from each of the three major credit reporting bureaus by visiting [www.annualcreditreport.com](http://www.annualcreditreport.com), calling 877-322-8228, or contacting the three major credit bureaus directly at: **Equifax**, P.O. Box 105069, Atlanta, GA, 30348, 800-525-6285, [www.equifax.com](http://www.equifax.com); **Experian**, P.O. Box 2002, Allen, TX 75013, 888-397-3742, [www.experian.com](http://www.experian.com); **TransUnion**, P.O. Box 2000, Chester, PA 19016, 800-680-7289, [www.transunion.com](http://www.transunion.com). Potentially impacted individuals may also find information regarding identity theft, fraud alerts, security freezes and the steps they may take to protect their information by contacting the credit bureaus, the Federal Trade Commission or their state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; [www.identitytheft.gov](http://www.identitytheft.gov); 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

ADS has set up a call center to answer questions from those who might be impacted by this incident. The hotline may be reached at 888-757-1875, Monday through Friday, 9 a.m. to 9 p.m. EST. Additional information on how potentially impacted individuals can protect themselves can also be found at ADS’s website [www.atlanticdigestive.com](http://www.atlanticdigestive.com). Instances of known or suspected identity theft should also be reported to law enforcement or the individual’s state Attorney General.