Clark Hill

Jason M. Schwent
T (312) 985-5939
F (312) 517-7573
Email:jschwent@ClarkHill.com

Clark Hill
130 E. Randolph Street, Suite 3900
Chicago, Illinois 60601
T (312) 985-5900
F (312) 985-5999

December 27, 2021

Sent via Online Portal

Attorney General Aaron Frey
Office of the Attorney General
6 State House Station
August, ME 04333

Dear Attorney General Aaron Frey:

We represent Florida Digestive Health Specialists, LLP ("FDHS") with respect to a data security incident involving the potential exposure of certain protected health information ("PHI") described in more detail below. FDHS is gastroenterology healthcare provider located in Bradenton, Florida. FDHS is committed to answering any questions you may have about the data security incident, its response, and steps taken to prevent a similar incident in the future.

1. Nature of security incident.

On December 16, 2020, an employee noted suspicious activity within their FDHS email account that resulted in suspicious emails having been sent from their employee account. Several days later, on December 21, 2020, FDHS learned that funds had been misrouted to an unknown bank account. FDHS immediately began an investigation to determine how the incident occurred, and what could be done to better protect our systems. FDHS also engaged Clark Hill PLC ("Counsel") to assist in the investigation of this incident and at Counsel's direction, engaged a nationally-recognized, third-party computer forensics firm, Kivu, to further assist in the investigation. The investigation found that a limited number of FDHS employee email accounts had been accessed by unauthorized users. That investigation was involved and, though access was confined to a limited number of FDHS email accounts, those accounts were voluminous. FDHS investigated those email accounts to determine what information was found in those accounts, whether it constituted personal information, protected health information, or other confidential information, and to whom that information belonged. This process took a considerable amount of time and only concluded on November 19, 2021.

2. Number of residents affected.

Eleven (11) Maine residents may have been affected and were notified of the incident. A notification letter was sent to the potentially affected individuals on December 27, 2021 (a copy of the form notification letter is enclosed as Exhibit A).

3. Steps taken in response to the incident.

FDHS took steps to address this incident and prevent similar incidents in the future. FDHS changed passwords and implemented multi-factor authentication throughout its IT systems. In addition, FDHS strengthened password protocols and reconfigured its firewall. Affected individuals were offered 12 months of credit monitoring and identity protection services through IDX.

4. Contact information.

FDHS takes the security of the information in its control seriously and is committed to ensuring information within its control is protected. If you have any questions or need additional information, please do not hesitate to contact me at jschwent@clarkhill.com or (312) 985-5939.

Sincerely,

CLARK HILL

Jason M. Schwent
Senior Counsel

cc: Mariah Leffingwell – mleffingwell@clarkhill.com

EXHIBIT A

Florida Digestive Health Specialists

P.O. Box 1907
Suwanee, GA 30024

To Enroll, Please Call:
1-833-365-2604
Or Visit:
https://response.idx.us/fdhs
Enrollment Code: <<XXXXXXXX>>

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

December 27, 2021

Notice of Data Breach

Dear <<First Name>> <<Last Name>>:

Florida Digestive Health Specialists, LLP ("FDHS") experienced a data security incident that may have impacted your protected health information ("PHI"). Specifically, the incident in question may have resulted in the disclosure of your name and medical information. We take the privacy and security of information involving our patients seriously, and sincerely apologize for any concern or inconvenience this may cause you. This letter contains information about steps you can take to protect your information and resources we are making available to help you.

1. Nature of security incident.

On December 16, 2020, an employee noted suspicious activity within their FDHS email account that resulted in suspicious emails having been sent from their employee account. Several days later, on December 21, 2020, FDHS learned that funds had been misrouted to an unknown bank account. FDHS immediately began an investigation to determine how the incident occurred, and what could be done to better protect our systems. We also engaged Clark Hill PLC ("Counsel") to assist in the investigation of this incident and at Counsel's direction, engaged a nationally-recognized, third-party computer forensics firm, Kivu, to further assist in the investigation. The investigation found that a limited number of FDHS employee email accounts had been accessed by unauthorized users. That investigation was involved and, though access was confined to a limited number of FDHS email accounts, those accounts were voluminous. FDHS investigated those email accounts to determine what information was found in those accounts, whether it constituted personal information, protected health information, or other confidential information, and to whom that information belonged. This process took a considerable amount of time and only concluded on November 19, 2021.

2. What information was involved?

The categories of PHI present in the posted data set include your first and last name, address, date of birth, Social Security number, financial information, health insurance information, medical information, diagnosis, health insurance individual policy number, and Medicare/Medicaid information.

3. What are we doing?

To further enhance security since this incident, FDHS has reset passwords, enabled multi-factor authentication in our email environment, and other enhanced security protocols. FDHS has also re-trained its employees on the proper handling of protected health information.

In addition, as a safeguard, we are offering identity theft protection services through IDX, the data breach and recovery services expert, at no charge to you. IDX identity protection services include: <<12 months/24 months>> of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With

this protection, IDX will help you resolve issues if your identity is compromised. Enroll in free identity protection services by calling 1-833-365-2604 or going to https://response.idx.us/fdhs and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Standard Time. Please note the deadline to enroll is March 27, 2022.

Additionally, in response to this incident, FDHS has taken steps to increase the security of its systems including, resetting passwords, enabling multi-factor authentication throughout our IT systems, and other enhanced safety protocols. We also deployed additional security controls, strengthened password protocols, and reconfigured our firewall.

4. What can you do?

It is always a good idea to review your bank account and other financial statements, and immediately contact your financial institution if you identify suspicious activity. We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling 1-833-365-2604 or going to https://response.idx.us/fdhs and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is March 27, 2022.

Additional information about protecting your identity is included in this letter, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file. We also encourage you to review your account statements and explanation of benefits, and to monitor your credit report for suspicious activity.

For More Information

You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Please call 1-833-365-2604 or go to https://response.idx.us/fdhs for assistance or for any additional questions you may have.

Sincerely,

Florida Digestive Health Specialists, LLP

Recommended Steps to help Protect your Information

1. **Website and Enrollment.** Go to https://response.idx.us/fdhs and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection 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, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-833-365-2604 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity 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. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you

will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

District of Columbia: Office of the Attorney General, 400 6th Street, NW, Washington, DC 20001; 202-727-3400; oag@dc.gov.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601**,** www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland**,** Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202**,** www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

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. You can 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.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

North Carolina Residents: Office of the Attorney General of North Carolina**,** 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400. You have the right to obtain any police report filed in regard to this incident. There were 14 Rhode Island residents impacted by this incident.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.

Florida Digestive Health Specialists

P.O. Box 1907
Suwanee, GA 30024

The Estate of
<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

December 27, 2021

Notice of Data Breach

To The Estate of <<First Name>> <<Last Name>>:

Florida Digestive Health Specialists, LLP ("FDHS") experienced a data security incident that may have impacted protected health information ("PHI") of your loved one. Specifically, the incident in question may have resulted in the disclosure of your loved one's name and medical information. We take the privacy and security of information involving our patients seriously, and sincerely apologize for any concern or inconvenience this may cause you. This letter contains information about steps you can take to protect your loved one's information and resources we are making available to help you.

1. Nature of security incident.

On December 16, 2020, an employee noted suspicious activity within their FDHS email account that resulted in suspicious emails having been sent from their employee account. Several days later, on December 21, 2020, FDHS learned that funds had been misrouted to an unknown bank account. FDHS immediately began an investigation to determine how the incident occurred, and what could be done to better protect our systems. We also engaged Clark Hill PLC ("Counsel") to assist in the investigation of this incident and at Counsel's direction, engaged a nationally-recognized, third-party computer forensics firm, Kivu, to further assist in the investigation. The investigation found that a limited number of FDHS employee email accounts had been accessed by unauthorized users. That investigation was involved and, though access was confined to a limited number of FDHS email accounts, those accounts were voluminous. FDHS investigated those email accounts to determine what information was found in those accounts, whether it constituted personal information, protected health information, or other confidential information, and to whom that information belonged. This process took a considerable amount of time and only concluded on November 19, 2021.

2. What information was involved?

The categories of PHI present in the posted data set include your loved one's first and last name, address, date of birth, Social Security number, financial information, health insurance information, medical information, diagnosis, health insurance individual policy number, and Medicare/Medicaid information.

3. What are we doing?

To further enhance security since this incident, FDHS has reset passwords, enabled multi-factor authentication in our email environment, and other enhanced security protocols. FDHS has also re-trained its employees on the proper handling of protected health information.

Additionally, in response to this incident, FDHS has taken steps to increase the security of its systems including, resetting passwords, enabling multi-factor authentication throughout our IT systems, and other enhanced safety protocols. We also deployed additional security controls, strengthened password protocols, and reconfigured our firewall.

4. What can you do?

It is always a good idea to review your loved one's bank account and other financial statements, and immediately contact their financial institution if you identify suspicious activity.

Additional information about protecting your loved one's identity is included in this letter, including recommendations by the Federal Trade Commission regarding identity theft protection. We also encourage you to review your loved one's account statements and explanation of benefits, and to monitor your loved one's credit report for suspicious activity.

For More Information

If you have any questions or concerns, please call 1-833-365-2604 for assistance or for any additional questions you may have. Your trust is our top priority, and we deeply regret any inconvenience or concern this matter may cause you.

Sincerely,

Florida Digestive Health Specialists, LLP

Recommended Steps to help Protect your Information

You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

District of Columbia: Office of the Attorney General, 400 6th Street, NW, Washington, DC 20001; 202-727-3400; oag@dc.gov.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601**,** www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland**,** Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202**,** www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

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. You can 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.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

North Carolina Residents: Office of the Attorney General of North Carolina**,** 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400. You have the right to obtain any police report filed in regard to this incident. There were 14 Rhode Island residents impacted by this incident.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.

Florida Digestive Health Specialists

P.O. Box 1907
Suwanee, GA 30024

Parent or Guardian of
<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

December 27, 2021

Notice of Data Breach

Dear Parent or Guardian of <<First Name>> <<Last Name>>:

Florida Digestive Health Specialists, LLP ("FDHS") experienced a data security incident that may have impacted your child's protected health information ("PHI"). Specifically, the incident in question may have resulted in the disclosure of your child's name and medical information. We take the privacy and security of information involving our patients seriously, and sincerely apologize for any concern or inconvenience this may cause you or your child. This letter contains information about steps you can take to protect your child's information and resources we are making available to help you and your child.

1. Nature of security incident.

On December 16, 2020, an employee noted suspicious activity within their FDHS email account that resulted in suspicious emails having been sent from their employee account. Several days later, on December 21, 2020, FDHS learned that funds had been misrouted to an unknown bank account. FDHS immediately began an investigation to determine how the incident occurred, and what could be done to better protect our systems. We also engaged Clark Hill PLC ("Counsel") to assist in the investigation of this incident and at Counsel's direction, engaged a nationally-recognized, third-party computer forensics firm, Kivu, to further assist in the investigation. The investigation found that a limited number of FDHS employee email accounts had been accessed by unauthorized users. That investigation was involved and, though access was confined to a limited number of FDHS email accounts, those accounts were voluminous. FDHS investigated those email accounts to determine what information was found in those accounts, whether it constituted personal information, protected health information, or other confidential information, and to whom that information belonged. This process took a considerable amount of time and only concluded on November 19, 2021.

2. What information was involved?

The categories of PHI present in the posted data set include your child's first and last name, address, date of birth, Social Security number, financial information, health insurance information, medical information, diagnosis, health insurance individual policy number, and Medicare/Medicaid information.

3. What are we doing?

To further enhance security since this incident, FDHS has reset passwords, enabled multi-factor authentication in our email environment, and other enhanced security protocols. FDHS has also re-trained its employees on the proper handling of protected health information.

Additionally, in response to this incident, FDHS has taken steps to increase the security of its systems including, resetting passwords, enabling multi-factor authentication throughout our IT systems, and other enhanced safety protocols. We also deployed additional security controls, strengthened password protocols, and reconfigured our firewall.

4. What can you do?

Information about protecting your child's identity is included in this letter. We also encourage you to review your child's account statements and explanation of benefits for suspicious activity.

For More Information

If you have any questions or concerns, please call 1-833-365-2604 for assistance or for any additional questions you may have. Your trust is our top priority, and we deeply regret any inconvenience or concern this matter may cause you.

Sincerely,

Florida Digestive Health Specialists, LLP

Recommended Steps to help Protect your Information

You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

District of Columbia: Office of the Attorney General, 400 6th Street, NW, Washington, DC 20001; 202-727-3400; oag@dc.gov.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601**,** www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland**,** Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202**,** www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

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. You can 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.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

North Carolina Residents: Office of the Attorney General of North Carolina**,** 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400. You have the right to obtain any police report filed in regard to this incident. There were 14 Rhode Island residents impacted by this incident.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.