Exhibit A

Florida Digestive Health Specialists, LLP
PO Box 1286
Dearborn, MI 48120-9998

[redacted]

August 13, 2024

Dear [redacted]:

We wanted to let you know about a recent data security incident that may have impacted your protected health information ("PHI"). Florida Digestive Health Specialists, LLP ("FDHS") takes the privacy and security of all patient information seriously, and sincerely apologizes 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.

**What happened?**

On March 28, 2024, FDHS learned that PHI may have been taken from its systems. As soon as FDHS learned of this incident, it began an investigation to identify what occurred and what patient data may be at risk. FDHS also began working with independent cybersecurity specialists to help determine what had occurred. On April 30, 2024, in conjunction with law enforcement, FDHS was able to determine the scope of the information affected. Then, on June 14, 2024, the investigation concluded, and FDHS learned that some patient data may have been impacted. While we are not aware of any misuse of your information, we wanted to inform you of this incident as soon as possible.

**What information was involved?**

From our review, your name and the following information may have been impacted in this incident: <<Variable Text>>.

**What we are doing:**

We want to assure you that we have taken steps to prevent this kind of event from happening in the future. Since the incident, we performed a global password reset and made significant network changes to increase the security of our network.

In response to the incident, we are providing you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services provide you with alerts for 12 months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company, specializing in fraud assistance and remediation services.

**What you can do:**

It is always a good idea to remain vigilant for incident of identity theft or fraud, and to review your bank account and other financial statements as well as your credit reports for suspicious activity. We also encourage you to contact Cyberscout with any questions and to take full advantage of the Cyberscout service offering. 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.

**How do I enroll for the free services?**

To enroll in Credit Monitoring services at no charge, please log on to **https://bfs.cyberscout.com/activate** and follow the instructions provided. When prompted please provide the following unique code to receive services: [redacted]

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

**For more information:**

If you have any questions or concerns, please call TransUnion at **1-833-531-1388** Monday through Friday from 8am - 8pm Eastern time, excluding holidays. Your trust is our top priority, and we deeply regret any inconvenience or concern that this matter may cause you.

Sincerely,

*Florida Digestive Health Specialists LLP*

Florida Digestive Health Specialists LLP

**Recommended steps to help protect your information**

***You've been provided with access to the following services from Cyberscout:***

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

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

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

**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.

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
P.O. Box 105069
Atlanta, GA 30348-5069

Equifax Credit Freeze
P.O. Box 105788
Atlanta, GA 30348-5788
1-888-836-6351
www.equifax.com/personal/credit-report-services

Experian Fraud Reporting and Credit Freeze
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion Fraud Reporting
P.O. Box 2000
Chester, PA 19022-2000

TransUnion Credit Freeze
P.O. Box 160
Woodlyn, PA 19094
1-800-680-7289
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.

**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/201904_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 are 2 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