EXHIBIT 1

By providing this notice, Spokane Digestive Disease Center, P.S. ("SDDC") does not waive any rights or defenses regarding the applicability of Washington law, the applicability of the Washington data event notification statute, or personal jurisdiction.

Nature of the Data Event

On February 19, 2026, SDDC became aware of suspicious activity related to one (1) employee's email account. SDDC took measures to secure its email environment to mitigate the risk of further activity and launched an investigation to determine the nature and scope of the activity. The investigation determined that an unauthorized actor accessed a SDDC email account between January 22, 2026, and February 18, 2026. SDDC then performed a comprehensive review of the accessed emails and attachments to determine what information was at issue and to whom the information relates. On May 8, 2026, we completed this process, and SDDC worked to issue notification.

The information that could have been subject to unauthorized access for Washington residents includes name, date of birth, driver's license number or state identification card number, Social Security number, financial account information, credit card information, electronic signature, and/or medical information.

Notice to Washington Residents

On May 26, 2026, SDDC provided written notice of this incident to two thousand ninety three (2,093) Washington residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon learning of the event, SDDC moved to investigate and respond to the incident, assess the security of SDDC's email environment, and identify potentially affected individuals. SDDC is also working to implement additional safeguards and additional training to its employees to reduce the likelihood of a similar future event. SDDC is providing access to credit monitoring services for one (1) year through Experian to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, SDDC is providing potentially impacted individuals with guidance on how to better protect against identity theft and fraud as well as providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and 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.

SDDC is providing written notice of this incident to relevant state regulators, as necessary. SDDC is also notifying the U.S. Department of Health and Human Services and prominent media pursuant to the Health Insurance Portability and Accountability Act (HIPAA).

EXHIBIT A

spokane digestive CENTER

Return Mail Processing
PO Box 999
Suwanee, GA 30024

12 1 2212 **********AUTO**5-DIGIT 99208
SAMPLE A. SAMPLE - L01
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

May 26, 2026

[Extra3]

Dear Sample A. Sample:

Spokane Digestive Disease Center, P.S. ("SDDC") is writing to notify you of an event that may affect the privacy of some of your information. We take this event very seriously and the confidentiality, privacy, and security of information in our care is one of our highest priorities. While we are not aware of any actual or attempted identity theft or fraud in connection with this event, this letter provides an overview of the event, our response, and steps you may take to help protect your information, should you feel it appropriate to do so.

What Happened? On February 19, 2026, we became aware of suspicious activity related to an employee's email account. We took measures to secure our email environment to mitigate the risk of further activity, and launched an investigation to determine the nature and scope of the activity. The investigation determined that an unauthorized actor accessed a SDDC email account on certain dates between January 22, 2026, and February 18, 2026. We then performed a comprehensive review of the potentially accessed emails and attachments to determine what information was at issue and to whom the information relates. We recently completed the review, and determined that your information was contained in the emails reviewed.

What Information Was Involved? The following types of information related to you were present in the potentially affected emails: [Extra1].

What We Are Doing. Upon learning of the event, we secured the account and initiated an investigation into the event. As part of our ongoing commitment to the privacy of information in our care, we are working to implement additional safeguards and additional training to our employees to reduce the likelihood of a similar future event. We are providing written notice of this event to relevant state regulators, as necessary, as well as notifying the U.S. Department of Health and Human Services pursuant to the Health Insurance Portability and Accountability Act (HIPAA).

As an added precaution, we are offering you immediate access to 12 months of complimentary credit monitoring and identity theft protection services through Experian. You can find information on how to enroll in these services in the enclosed *Steps You Can Take To Protect Personal Information*. We encourage you to enroll yourself in these services as we are not able to do so on your behalf.

What You Can Do. You can review the enclosed *Steps You Can Take to Protect Personal Information* which contains guidance regarding steps you can take to protect against possible misuse of your information. Though we have no indication of any identity theft or fraud in connection with this event, we also encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. Any suspicious activity should be promptly reported to the appropriate health care provider, insurance company, or financial institution. You may also enroll in the complimentary credit monitoring and identity theft protection services we are offering.

For More Information. We understand that you may have questions about this event that are not addressed in this letter. If you have additional questions or need assistance, please call 1-833-918-7291 Monday through Friday from 6 am to 6 pm Pacific Time, excluding holidays. You may also write to SDDC at 105 W 8th Ave, Suite 6010, Spokane, WA 99204.

Sincerely,

Spokane Digestive Disease Center, P.S.

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Monitoring Services

To help protect your identity, we are offering complimentary access to Experian IdentityWorks[SM] for [Extra2] months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for [Extra2] months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary [Extra2]-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by** August 31, 2026 by 11:59 pm UTC (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: www.experianidworks.com/1Bcredit
- Provide your **activation code**: ABCDEFGHI

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team by August 31, 2026 at 1-833-918-7291 Monday - Friday, 6 am - 6 pm Pacific Time (excluding major U.S. holidays). Be prepared to provide engagement number [Engagement Number] as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR [Extra2]-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance:** Provides coverage for certain costs and unauthorized electronic fund transfers.

[1] Offline members will be eligible to call for additional reports quarterly after enrolling.
[2] The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/data-breach-help
1-888-298-0045	1-888-397-3742	1-833-799-5355
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

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

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

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