EXHIBIT 1

We write to notify your office on behalf of the entities identified in ***Exhibit A***, collectively referred to as the "Notifying Entities" in this notification, of an incident that may affect the security of certain personal information relating to seven (7) Maine residents. This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Advanced Medical Practice Management ("AMPM") and the Notifying Entities do not waive any rights or defenses regarding the applicability of Maine law, the applicability of the Maine data event notification statute, or personal jurisdiction.

Nature of the Data Event

AMPM is a third-party billing administrator that provides billing services to certain healthcare providers, including the Notifying Entities.

On August 5, 2021, AMPM became aware of suspicious activity associated with certain files within its network. AMPM quickly took steps to secure its network and began an investigation, which was aided by third-party forensic specialists, to determine the nature and scope of the activity. AMPM's investigation subsequently determined that an unauthorized actor acquired certain files from its environment between July 11, 2021, and July 13, 2021. Given that these certain files were accessed without authorization, AMPM then began a comprehensive review of the contents of the files, again aided by third-party specialists, to determine the information potentially impacted by this incident, and to whom the information related for purposes of providing notification. AMPM completed this review on December 3, 2021, and determined that information associated with the above covered entities was present in the files at the time of the incident. Once the review was complete, AMPM worked diligently to reconcile this information with its internal records to confirm the individuals whose information may have been affected and the appropriate contact information for those individuals.

AMPM completed these efforts and began providing notice to relevant healthcare providers whose patients were potentially impacted, including the Notifying Entities, on January 27, 2022. These notification efforts were completed on January 28, 2022. Since then, AMPM has been working collaboratively with the relevant healthcare providers, including the Notifying Entities, to notify the impacted individuals regarding the incident at the providers' direction.

The information maintained by AMPM associated with the Notifying Entities that may have been subject to unauthorized access varies by individual but includes the following: name, Social Security number, driver's license number or state identification equivalent, and financial account information.

Notice to Maine Residents

On or about March 23, 2022, AMPM began providing written notice of this incident to affected individuals, which includes seven (7) Maine residents. Written notice is being provided in substantially the same form as the letters attached hereto as ***Exhibit B***.

Other Steps Taken and To Be Taken

Upon discovering the event, AMPM moved quickly to investigate and respond to the incident, assess the security of AMPM systems, and identify potentially affected healthcare providers and individuals. Further, AMPM promptly notified federal law enforcement regarding this event. AMPM is also reviewing and enhancing its existing policies and procedures relating to data protection and security, implementing additional security measures and safeguards to protect against this type of event in the future, and also providing additional training to employees. Additionally, as an added measure, AMPM is also providing access to credit monitoring services for twelve (12) months through Kroll to individuals whose Social Security number, driver's license number or state identification equivalent, passport number, or other government-issued identification number was potentially affected by this incident, at no cost to these individuals. Moreover, at the direction of the Notifying Entities, AMPM is notifying other relevant state and federal regulatory authorities, as required.

Additionally, AMPM is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including 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.

EXHIBIT A

Notifying Entities

- Affiliates in Gastroenterology
- The Florham Park Endoscopy ASC, LLC
- The Hanover NJ Endoscopy ASC, LLC

EXHIBIT B

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

RE: NOTICE OF DATA EVENT

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

Advanced Medical Practice Management ("AMPM") is a third-party medical billing administrator that provides billing services to certain healthcare providers, including <<b2b_text_1 (Covered Entity)>>. AMPM is writing on behalf of <<b2b_text_1 (Covered Entity)>>, to notify you of a recent event at AMPM that may have affected the privacy of some of your personal information. This notice provides information about the incident, our response, and resources available to you to help protect your information from possible misuse, should you feel it appropriate to do so.

What Happened? On August 5, 2021, AMPM discovered suspicious activity associated with certain files within our environment. AMPM quickly took steps to secure the network, and began an investigation to determine the nature and scope of the activity. Our investigation subsequently determined that an unauthorized actor acquired certain files from our environment between July 11, 2021 and July 13, 2021. Given that these certain files were accessed without authorization, we then began a comprehensive review of the files to determine the information potentially impacted by this incident and to whom the information related for purposes of notification. Upon completion of this review, we then worked diligently to reconcile this information with our internal records to confirm the individuals whose information may have been affected and the appropriate contact information for those individuals. We completed this review on January 27, 2022, and thereafter worked to provide notification to organizations whose patients were potentially impacted, including <<b2b_text_1 (Covered Entity)>>, in order to obtain necessary information and approval, and thereafter began notifying potentially impacted individuals as quickly as possible. We are notifying you out of an abundance of caution because your information was determined to be present in one of the specific files involved, and therefore may have been accessed during this incident.

What Information Was Involved? Our investigation determined that the impacted information may include your <<b2b_text_2 ("name" and Data Elements)>>. While we have no evidence of any actual or attempted misuse of your information, we are letting you know out of an abundance of caution and providing information and resources to assist you in helping to protect your personal information, should you feel it appropriate to do so.

What We Are Doing. AMPM treats its responsibility to safeguard information in its possession as an utmost priority. As such, we responded quickly to this event and have been working diligently to provide you with an accurate and complete notice of the incident. Our response to this event also included prompt reporting to federal law enforcement. Further, as part of our ongoing commitment to the privacy and security of personal information in our care, we are reviewing and enhancing our existing policies and procedures relating to data protection and security. We have also instituted additional security measures, as well as provided additional training to employees, to mitigate any risk associated with this incident and to better protect against future incidents. We are also notifying relevant state and federal regulators, as required.

As an added precaution we are offering you access to 12 months of identity monitoring services through Kroll at no cost to you. If you wish to activate these services, you may follow the instructions included in the attached *Steps You Can Take to Help Protect Personal Information*. We encourage you to activate these services as we are unable to act on your behalf to do so.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account and monitoring your free credit reports for suspicious activity and to detect errors. Further, please review the enclosed "*Steps You Can Take to Help Protect Personal Information*" section of the letter for additional information. You can also activate the complimentary identity monitoring services that we are offering to you.

For More Information. We understand that you may have questions that are not addressed in this notice. If you have additional questions or concerns, please call our dedicated call center at [XXX-XXX-XXXX], which is available from 8:00 a.m. to 5:30 p.m. Central Time, Monday through Friday, excluding some U.S. holidays. Please have your membership number ready.

Sincerely,

Advanced Medical Practice Management

Steps You Can Take to Help Protect Personal Information

Activate Identity Monitoring

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6 (Activation Date)>> to activate your identity monitoring services.

Membership Number: **<<Membership Number s_n>>**

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

If you prefer to activate these services offline and receive monitoring alerts via the US Postal Service, you may activate via our automated phone system by calling 1-888-653-0511, Monday through Friday, 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays. Please have your membership number located in your letter ready when calling. Please note that to activate monitoring services, you will be required to provide your name, date of birth, and Social Security number through our automated phone system.

Additional information describing your services is included with this letter.

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 your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your 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 you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one 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 your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide 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 you are a victim of identity theft.

Should you wish to place a credit freeze, 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/credit-help
888-298-0045	888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, 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 Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a

complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag@dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us. AMPM is located at 25B Hanover Road #250, Florham Park, NJ 07932.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus 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 violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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/.

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 Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There is/are approximately [#] Rhode Island residents impacted by this incident.

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

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 Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud 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.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll 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 will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

RE: NOTICE OF DATA EVENT

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

Advanced Medical Practice Management ("AMPM") is a third-party medical billing administrator that provides billing services to certain healthcare providers, including <<b2b_text_1 (Covered Entity)>>. AMPM is writing on behalf of <<b2b_text_1 (Covered Entity)>>, to notify you of a recent event at AMPM that may have affected the privacy of some of your personal information. This notice provides information about the incident, our response, and resources available to you to help protect your information from possible misuse, should you feel it appropriate to do so.

What Happened? On August 5, 2021, AMPM discovered suspicious activity associated with certain files within our environment. AMPM quickly took steps to secure the network, and began an investigation to determine the nature and scope of the activity. Our investigation subsequently determined that an unauthorized actor acquired certain files from our environment between July 11, 2021 and July 13, 2021. Given that these certain files were accessed without authorization, we then began a comprehensive review of the files to determine the information potentially impacted by this incident and to whom the information related for purposes of notification. Upon completion of this review, we then worked diligently to reconcile this information with our internal records to confirm the individuals whose information may have been affected and the appropriate contact information for those individuals. We completed this review on January 27, 2022, and thereafter worked to provide notification to organizations whose patients were potentially impacted, including <<b2b_text_1 (Covered Entity)>>, in order to obtain necessary information and approval, and thereafter began notifying potentially impacted individuals as quickly as possible. We are notifying you out of an abundance of caution because your information was determined to be present in one of the specific files involved, and therefore may have been accessed during this incident.

What Information Was Involved? Our investigation determined that the impacted information may include your <<b2b_text_2 ("name" and Data Elements)>>. While we have no evidence of any actual or attempted misuse of your information, we are letting you know out of an abundance of caution and providing information and resources to assist you in helping to protect your personal information, should you feel it appropriate to do so.

What We Are Doing. AMPM treats its responsibility to safeguard information in its possession as an utmost priority. As such, we responded quickly to this event and have been working diligently to provide you with an accurate and complete notice of the incident. Our response to this event also included prompt reporting to federal law enforcement. Further, as part of our ongoing commitment to the privacy and security of personal information in our care, we are reviewing and enhancing our existing policies and procedures relating to data protection and security. We have also instituted additional security measures, as well as provided additional training to employees, to mitigate any risk associated with this incident and to better protect against future incidents. We are also notifying relevant state and federal regulators, as required.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account and monitoring your free credit reports for suspicious activity and to detect errors. Further, please review the enclosed "*Steps You Can Take to Help Protect Personal Information*" section of the letter for additional information.

For More Information. We understand that you may have questions that are not addressed in this notice. If you have additional questions or concerns, please call our dedicated call center at [XXX-XXX-XXXX], which is available from 8:00 a.m. to 5:30 p.m. Central Time, Monday through Friday, excluding some U.S. holidays.

Sincerely,

Advanced Medical Practice Management

Steps You Can Take to Help Protect Personal Information

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 your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your 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 you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one 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 your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide 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 you are a victim of identity theft.

Should you wish to place a credit freeze, 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/credit-help
888-298-0045	888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, 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 Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

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

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag@dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us. AMPM is located at 25B Hanover Road #250, Florham Park, NJ 07932.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus 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 violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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/.

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 Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There is/are approximately [#] Rhode Island residents impacted by this incident.