Genesis Billing Services, Inc
c/o Cyberscout
<<Return Address>>
<<City>>, <<State>> <<Zip>>

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<PostalCode+4>>

September 5, 2025

Notice of Data Incident

Dear <<First Name>> <<Last Name>>,

What Happened

We are contacting you regarding a data incident that occurred on or about May 20, 2025 at Genesis Billing Services, Inc. ("Genesis") in North Carolina. As a result of this security incident, some of your personal information may have been exposed to others. While we are not aware of any additional evidence indicating that your information has been taken or used for fraudulent purposes, we are unable to conclusively rule out the possibility that your personal information was compromised as a result of this incident. Therefore, out of an abundance of caution, we are notifying you of this incident.

What Happened

At Keys Pathology Associates, PA ("Keys Pathology"), we utilized a vendor, Genesis, to host our patient data on a third-party server for billing purposes. We do not have access to nor control of this server. On May 27, 2025, Genesis informed us that an unknown actor accessed the server used to host Keys Pathology data without authorization around May 20, 2025. According to Genesis, an unknown threat actor downloaded all of Genesis's files and encrypted their entire system. Genesis also indicated that it had notified federal law enforcement of the incident.

On August 21, 2025, we were able to begin deciphering the names and contact information of potentially affected patients from an unstructured data file we had received. We have been diligently working through this supplied information and have now determined your information was included within Genesis's affected server. We are notifying you of this incident at this time.

What Information Was Involved

Although the specific information that was contained within the server varies by individual, according to the investigation performed by Genesis, such information may include: first and last name, address, date of birth, phone number, address, Social Security number, driver's license number, and health information.

What We Are Doing

At Keys Pathology, we take the responsibility of maintaining non-public patient information seriously, which is a major reason why we utilized the services of a professional provider like Genesis to host our patient data. We will no longer utilize Genesis for our professional services in an effort to reduce the risk of a similar incident occurring again. In addition, we are offering a Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for <<Service Length>> 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

We encourage you to contact TransUnion with any questions and to enroll in the free identity protection services by calling 1-833-426-7791 between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays, going to **https://bfs.cyberscout.com/activate** or scanning the QR image and using the Enrollment Code provided above. Please note the deadline to enroll is 90 days from the date of this letter.

Again, at this time, we are not aware of any additional evidence indicating that your information has been obtained or misused. However, we encourage you to take full advantage of this service offering.

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.

We deeply regret that this has occurred and apologize for any inconvenience or concern caused by this incident. Please call 1-833-426-7791 if you'd like to speak to someone.

Sincerely,

Dr. Zhiming Li

Dr. Zhiming Li
President
Keys Pathology Associates, PA

(Enclosure)

Recommended Steps to Help Protect Your Information

1. **Website and Enrollment.** Scan the QR image or go to **https://bfs.cyberscout.com/activate** 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 TransUnion 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, TransUnion will be able to assist you.

3. Telephone. Contact TransUnion at 1-833-426-7791 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 TransUnion identity protection, notify them immediately by calling or by logging into the TransUnion website and filing a request for help.

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. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

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 Maryland Attorney General and Consumer Protection Division at 200 Saint Paul Place, Baltimore, Maryland, 21202, www.marylandattorneygeneral.gov or call 410-576-6337.

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: 1-877-877-9392

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