<<Return to Kroll>>
<<Return Address>>
<<City, State ZIP>>

<<FIRST_NAME>> <<MIDDLE_NAME>> <<LAST_NAME>> <<SUFFIX>>
<<ADDRESS_1>>
<<ADDRESS_2>>
<<CITY>>, <<STATE_PROVINCE>> <<POSTAL_CODE>>
<<COUNTRY>>

SCAN TO ENROLL

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

NOTICE OF DATA BREACH

Dear <<First_name>> <<Last_name>>:

Information security is a top priority for Vital Imaging Diagnostic Centers LLC, which is why we are writing to inform you of security breach involving your personal information. Despite our security safeguards and controls in place, we experienced this incident and are providing you with details about the isolated incident, our response, and additional steps you may take to protect your information, should you choose to do so. You are receiving this notice because you are a current or former employee, or you are a dependent of a current or former employee.

What Happened? On February 13, 2025, Vital Imaging became aware of unauthorized activity on our network. In response, we partnered with an outside IT security firm to investigate the incident. We later determined that certain files were removed from our network without our authorization. We commenced a detailed and time-consuming review of the data involved, to understand whether those files contained personal information, and if so, to whom the information belonged. We concluded our review, analysis of the data, and identification of last known address information on February 19, 2026. We are now notifying the individuals whose information was involved, yet we stress that we have received no reports of any fraud or misuse of information at any time since the incident occurred.

What Information Was Involved? The information includes your first and last name, in combination with the following data element(s): <<b2b_text_1 (data elements)>>.

What We Are Doing. Upon identifying the unauthorized activity, we partnered with specialists to confirm our network was secure and investigate whether any data was removed. Once we confirmed, we reported the incident to law enforcement, and commenced our detailed review. Additionally, we continue to assess our existing security safeguards and policies for ways to remain resilient against evolving threats.

As an added precaution, we are providing you with identity monitoring services through Kroll for <<ServiceTerminMonths>> months. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

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

*You have until **<<b2b_text_6 (activation deadline)>>** to activate your identity monitoring services.*

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

What You Can Do. We reiterate that we have no reports of identity fraud or fraudulent activity involving your information as a result of this incident. However, we encourage you to remain vigilant against incidents of identity theft and fraud, from any source, by reviewing your credit reports and account statements and explanations of benefits (EOBs) for suspicious activity and to detect errors. If you discover any suspicious or unusual activity on your accounts, please promptly contact your financial institution or the service provider. Please refer to the enclosed "*Steps You Can Take to Help Protect Your Information*" for additional resources you may take advantage of to protect your information.

For More Information. Should you have any questions or concerns, please contact our professional assistance line with Kroll call center at (844) 403-4506, Monday through Friday, 8:00 AM to 5:30 PM Central Time, excluding major U.S. holidays. For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

We remain committed to protecting your trust in us and continue to be thankful for your support and understanding.

Sincerely,

Vital Imaging Diagnostic Centers LLC

Enclosure: *Steps You Can Take to Help Protect Your Information*

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Monitor Your Accounts and Credit Reports: It is good practice to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements and explanation of benefits forms for suspicious activity and to detect errors.

You May Obtain a Free Credit Report: Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit https://annualcreditreport.com, call toll-free at 1-877-322-8228, complete the Annual Credit Report Request Form on the Federal Trade Commission's (FTC) website at https://ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact one of the credit reporting bureaus.

Fraud Alert Services: You have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report at no cost, contact any of the three credit reporting agencies identified below.

Credit Freeze Instructions: As an alternative to a fraud alert, you 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 your 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 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 credit freeze, you should provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth;
4. Address information from the prior two to five years;
5. Proof of current address, such as current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver's license or identification card); 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 fraud alert or credit freeze, you may contact a major credit reporting bureau listed below:

TransUnion 1-800-680-7289 www.transunion.com	**Experian** 1-888-397-3742 www.experian.com	**Equifax** 1-888-298-0045 www.equifax.com
TransUnion Fraud Alert P.O. Box 2000 Chester, PA 19016-2000	**Experian Fraud Alert** P.O. Box 9554 Allen, TX 75013	**Equifax Fraud Alert** P.O. Box 105069 Atlanta, GA 30348-5069
TransUnion Credit Freeze P.O. Box 160 Woodlyn, PA 19094	**Experian Credit Freeze** P.O. Box 9554 Allen, TX 75013	**Equifax Credit Freeze** P.O. Box 105788 Atlanta, GA 30348-5788

Additional Information

This notice has not been delayed by law enforcement. If you experience identity theft or fraud, you have the right to file a police report with your local law enforcement agency. When filing a report, you may be required to provide documentation showing that you have been a victim, and you are entitled to obtain a copy of the report for your records. If you discover suspicious activity on your credit reports or otherwise believe your information is being misused, you should promptly contact local law enforcement to file a report.

Instances of known or suspected identity theft should also be reported to your state Attorney General and the FTC. A complaint may be filed with the FTC online at https://ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Complaints submitted to the FTC are added to its Identity Theft Data Clearinghouse and made available to law enforcement for investigative purposes. The FTC also provides information about fraud alerts and security freezes.

For D.C. residents, the District of Columbia Attorney General may be contacted at 400 6th Street, NW, Washington, D.C. 20001; (202) 4; 202-727-3400, and https://oag.dc.gov/consumer-protection.

For Maryland residents, the Maryland Attorney General may be contacted at Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202; 1-888-743-0023; or https://oag.dc.gov/consumer-protection.

For New York residents, the New York Attorney General may be contacted at 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; or https://ncdoj.gov.

You also have rights under the federal Fair Credit Reporting Act (FCRA) and Identity Security Act, which governs the collection and use of information pertaining to you by consumer reporting agencies. These rights include the right to access the information in your file, dispute incomplete or inaccurate information, and request correction or deletion of inaccurate, incomplete, or unverifiable information. For more information about the FCRA and your rights, you may visit www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf or https://ftc.gov.

You may contact Vital Imaging by mail at 7101 S.W. 99th Ave., Suite 106, Miami, Florida 33173 or by phone at 305.596.0942.