MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

February 16, 2024

VIA E-MAIL

Office of the New Hampshire Attorney General
Consumer Protection & Antitrust Bureau
33 Capitol Street
Concord, NH 03301
E-mail: DOJ-CPB@doj.nh.gov

Re: Notice of Data Event

To Whom It May Concern:

We represent Cardiothoracic and Vascular Surgeons, P.A. ("CTVS") located at 1010 West 40th Street, Austin, Texas 78756, and are writing to notify your office of an incident that may affect the security of certain personal information relating to approximately two (2) New Hampshire residents. By providing this notice, CTVS does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

On October 13, 2023, CTVS became aware of suspicious activity relating to its systems. CTVS immediately launched an investigation to determine the full nature and scope of the activity and to restore functionality to the impacted systems. The investigation determined that certain information stored within the CTVS environment was viewed or taken by an unauthorized actor between October 12, 2023 and October 13, 2023. Upon becoming aware of this information, CTVS began a diligent and comprehensive review process to identify sensitive information that was contained within the impacted files, and to identify the individuals whose information may have been impacted. CTVS then worked to identify appropriate contact information for the impacted individuals. That process completed on January 22, 2024. CTVS then provided written notification to impacted individuals whose information was contained within the impacted files.

The information that could have been subject to unauthorized access includes

.

Notice to New Hampshire Residents

On or about February 16, 2024, CTVS began providing written notice of this incident to approximately two (2) New Hampshire 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 discovering the event, CTVS moved quickly to investigate and respond, assess the security of CTVS systems, and identify potentially affected individuals. Further, CTVS notified federal law enforcement regarding the event. CTVS is also working to implement additional safeguards and training to its employees. CTVS is providing access to credit monitoring services for through TransUnion, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

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

CTVS is providing written notice of this incident to relevant state and federal regulators, as necessary. CTVS notified the U.S. Department of Health and Human Services, and also posted notification on its website.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at .

Very truly yours,

Edward J. Finn of
MULLEN COUGHLIN LLC

EJF/jrm
Enclosure

EXHIBIT A

Cardiothoracic and Vascular Surgeons, P.A.
c/o Cyberscout
1 Keystone Ave., Unit 700
Cherry Hill, NJ 08003
DB-08258 1-1

Cardiothoracic and Vascular Surgeons, P.A.

February 16, 2024

Notice of Security Incident

Dear :

Cardiothoracic and Vascular Surgeons, P.A. ("CTVS") is writing to notify you of a recent event that may impact the privacy of some of your information. Although at this time there is no indication that your information has been used to commit identity theft or fraud in relation to this event, we are providing you with information about the event, our response, and steps you may take to help protect your information, should you feel it necessary to do so.

What Happened? On October 13, 2023, CTVS became aware of suspicious activity relating to its systems. CTVS immediately launched an investigation to determine the full nature and scope of the activity and to restore functionality to the impacted systems. The investigation determined that certain information stored within our environment was viewed or taken by an unauthorized actor between October 12, 2023 and October 13, 2023. Upon becoming aware of this information, CTVS began a diligent and comprehensive review process to identify sensitive information that was contained within the impacted files, and to identify the individuals whose information may have been impacted. CTVS then worked to identify appropriate contact information for the impacted individuals. That process completed on January 22, 2024. We are notifying you because the investigation determined certain information related to you was contained within the impacted files.

What Information Was Involved? The review determined that the following information related to you was present in the impacted files: . At this time, we have no evidence that your information was subject to actual or attempted misuse as a result of this incident.

What We Are Doing. The confidentiality, privacy, and security of information within our care is among CTVS's highest priorities. Upon learning of the incident, we took immediate steps to secure our environment and investigate the activity. We also commenced an investigation to understand the nature and scope of the event. As part of our ongoing commitment to the privacy of information in our care, we are reviewing our policies, procedures, and processes related to the storage and access of sensitive information to reduce the likelihood of a similar future incident.

As an added precaution we are offering Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for twelve 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 through Identity Force, a TransUnion company specializing in fraud assistance and remediation services. Individuals who wish to receive these services must enroll by following the below enrollment instructions, as we are unable to activate them on your behalf.

What You Can Do. We 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 over the next . You can review the enclosed *Steps You Can Take to Help Protect Your Information* to learn helpful tips on steps you can take to protection against possible information misuse, should you feel it appropriate to do so. You may also enroll in the complimentary credit monitoring services we are offering to you.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, or need assistance, please call our dedicated assistance line at 833-791-2491, toll-free between the hours of 8:00 am to 8:00 pm Eastern time, Monday through Friday. You may also write to CTVS at 1010 West 40th Street, Austin, Texas 78756.

Sincerely,

Cardiothoracic and Vascular Surgeons, P.A.

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Enroll in Monitoring Services

To enroll in Credit Monitoring services at no charge, please log on to https://secure.identityforce.com/benefit/cardio and follow the instructions provided. When prompted please provide the following unique code to receive services:

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.

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/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
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

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 District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; (202) 442-9828; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/.

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 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, individuals have the right to obtain any police report filed in regard to this event. There are approximately 2 Rhode Island residents that may be impacted by this event.