MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

3 Allied Drive, Suite 303
Dedham, MA 02026

November 9, 2023

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 North Shore Medical Labs ("NSML") located at 463 Willis Avenue, Williston Park, NY 11596, and are writing to notify your office of an incident that may affect the security of certain personal information relating to approximately eight (8) New Hampshire residents. This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, NSML 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 or about March 29, 2023, NSML learned of a potential data security incident involving possible unauthorized access to certain computer systems. Upon learning of the potential incident, NSML quickly worked with external specialists to secure its systems and commenced an investigation to confirm the nature, scope, and impact of the incident. On May 12, 2023, the investigation determined that certain NSML data was potentially accessible to an unauthorized actor beginning on December 19, 2022. An unauthorized actor later used tools to copy certain data from NSML computers between March 17, 2023, and March 31, 2023. On May 26, 2023, NSML posted notice of the incident on its company website. NSML subsequently conducted a thorough review of the contents of the potentially affected data to determine whether the data contains any sensitive personal or medical information and if so, to whom the information relates. Upon conclusion of the review, NSML worked to notify affected individuals.

NSML has no indication that the data affected by this incident has been used to commit any identity theft, fraud, or other harm to individuals. The information that is present in the affected data includes: .

Notice to New Hampshire Residents

On or about November 9, 2023, NSML provided written notice of this incident to potentially affected individuals to approximately eight (8) New Hampshire residents. Written notice was provided in substantially the same form as the letter attached here as ***Exhibit A***. NSML is also providing notice of this incident on its website homepage to ensure all potentially affected individuals are notified.

Other Steps Taken and To Be Taken

Upon discovering the event, NSML moved quickly to investigate and respond to the event, assess the security of NSML systems, and identify potentially affected individuals. Further, NSML notified federal law enforcement regarding the event. NSML is also working to implement additional safeguards and training to its employees.

Additionally, NSML is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. NSML is providing individuals with information on how to place fraud alerts and credit freezes on their credit files, 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.

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

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,

Lynda Jensen of
MULLEN COUGHLIN LLC

LRJ/dle
Enclosure

EXHIBIT A

P.O. Box 1907
Suwanee, GA 30024

<<First Name>> <<Last Name>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip>>

November 9, 2023

<<Variable Header>>

Dear <<First Name>> <<Last Name>>:

North Shore Medical Labs ("NSML") writes to inform you of an incident that may affect the privacy of some of your information. Although NSML is unaware of any actual or attempted misuse of your information, NSML is providing you notice of the incident, steps NSML is taking in response, and resources available to help you better protect your information, should you feel it is appropriate to do so.

What Happened. On or about March 29, 2023, NSML learned of a potential data security incident involving possible unauthorized access to certain computer systems. Upon learning of the potential incident, NSML quickly worked with external specialists to secure its systems and commenced an investigation to confirm the nature, scope, and impact of the incident. On May 12, 2023, the investigation determined that certain NSML data was potentially accessible to an unauthorized actor beginning on December 19, 2022. An unauthorized actor later used tools to copy certain data from NSML computers between March 17, 2023, and March 31, 2023. NSML subsequently conducted a thorough review of the contents of the potentially affected data to determine whether the data contains any sensitive personal or medical information and if so, to whom the information relates. This review determined that your information was in the potentially affected data.

What Information Was Involved. NSML has no indication that the data affected by this incident has been used to commit any identity theft, fraud, or other harm to individuals. However, NSML is providing notice of this incident out of an abundance of caution because the information that is present in the affected data may include patient specific data including:
.

What We Are Doing. NSML takes very seriously its responsibility to safeguard the information it collects in providing services. As such, NSML responded immediately to this incident and is working diligently to provide accurate and complete notices of the incident as soon as possible to the appropriate individuals and entities. In addition, NSML notified law enforcement of the incident and continues to cooperate with the authorities' independent investigation efforts. As part of its ongoing commitment to the privacy and security of information in its care, NSML is reviewing its existing policies and training protocols relating to data protection. NSML also implemented enhanced security measures and monitoring tools to mitigate any risk associated with this incident and to better prevent similar incidents in the future. NSML is providing notice of this incident to potentially impacted individuals and to regulators where required.

What You Can Do. NSML sincerely regrets any inconvenience this incident may have caused. Although NSML is unaware of any misuse of information impacted by this incident, in accordance with best practices, individuals are encouraged to remain vigilant against incidents of identity theft and fraud by reviewing account statements, explanation of benefits, and free credit reports for unexpected activity or errors over the next . Any questionable activity detected should be reported to the associated insurance company, health care provider, or financial institution immediately.

For More Information. Individuals seeking additional information regarding this incident can call NSML's dedicated, toll-free number at , Monday through Friday, 9 am to 9 pm Eastern Time. Individuals may also write to NSML directly at: 463 Willis Avenue, Williston Park, NY 11596.

Sincerely,

North Shore Medical Labs

STEPS YOU CAN TAKE TO 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 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 one-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 you wish to place a fraud alert or 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
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; 1-202-727-3400; and oag.dc.gov.

For Massachusetts residents, Under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

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 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; 1-401-274-4400; and www.riag.ri.gov. Under Rhode Island law, individuals have the right to obtain any police report filed regarding this event. There are approximately <<six>> Rhode Island residents that may be impacted by this event.