



**MULLEN
COUGHLIN** LLC **CONSUMER PROTECTION**
ATTORNEYS AT LAW

RECEIVED

NOV 09 2021

Angelina W. Freind
Office: (267) 930-4782
Fax: (267) 930-4771
Email: afreind@mullen.law

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

November 4, 2021

VIA U.S. MAIL

Consumer Protection Bureau
Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Event

Dear Sir or Madam:

We represent Maxim Healthcare Group, including Maxim Healthcare Services and Maxim Healthcare Staffing (collectively "Maxim Healthcare") located at 7227 Lee Deforest Drive, Columbia, Maryland 21046 and are writing to notify your office of an incident that may affect the security of some personal information relating to two (2) New Hampshire residents. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Maxim Healthcare 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 December 4, 2020, Maxim Healthcare became aware of unusual activity related to several employees' email accounts. Maxim Healthcare immediately began an investigation to understand the nature and scope of this activity. The preliminary investigation revealed that a limited number of employees' email accounts were accessed without authorization between October 1, 2020 and December 4, 2020. Maxim Healthcare worked with outside forensic specialists to determine the full scope and impact of this event. Unfortunately, the investigation was not able to determine exactly which email messages or attachments may have been accessed or viewed without authorization. In an abundance of caution, a detailed and thorough programmatic and manual review of the contents of the email accounts was performed to determine whether sensitive information was contained in the email messages or attachments at the time of the incident. Upon receiving the initial results of the review, Maxim Healthcare worked diligently to locate address information and finalize the list of affected individuals. These efforts were completed on September 21, 2021.

The personal information that could have been subject to unauthorized access includes name, address, and Social Security number.

Mullen.law

Notice to New Hampshire Residents

On November 4, 2021, Maxim Healthcare provided written notice of this incident to affected individuals, which includes two (2) New Hampshire residents with personal information affected. Maxim Healthcare is also issuing notice to certain media outlets and posting notice of this incident on its website. 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, Maxim Healthcare moved quickly to investigate and respond to the incident, assess the security of Maxim Healthcare systems, and notify potentially affected individuals. Maxim Healthcare is also working to implement additional safeguards and training to its employees.

Additionally, Maxim Healthcare 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. Maxim Healthcare is 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. Maxim Healthcare is also notifying state and federal regulatory authorities, as required.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4782.

Very truly yours,

A handwritten signature in black ink, appearing to read 'AF', with a long horizontal line extending to the right.

Angelina W. Freind of
MULLEN COUGHLIN LLC

AWF/mah
Enclosure

EXHIBIT A

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

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

NOTICE OF DATA BREACH

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

Maxim Healthcare Group, including Maxim Healthcare Services and Maxim Healthcare Staffing (collectively “Maxim Healthcare”), writes to inform you of an incident that may affect the security 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 necessary to do so.

What Happened? On or about December 4, 2020, Maxim Healthcare became aware of unusual activity related to several employees’ email accounts. We immediately began to investigate to better understand the nature and scope of this activity. The preliminary investigation revealed that a limited number of employees’ email accounts were accessed without authorization between October 1, 2020 and December 4, 2020. We worked with outside forensic specialists to determine the full scope and impact of this event. Unfortunately, the investigation was not able to determine exactly which email messages or attachments may have been accessed or viewed without authorization. In an abundance of caution, a detailed and thorough programmatic and manual review of the contents of the email accounts was performed to determine whether sensitive information was contained in the email messages or attachments at the time of the incident. Upon receiving the initial results of the review on August 24, 2021, Maxim Healthcare worked diligently to locate address information for the affected individuals and completed that effort on September 21, 2021.

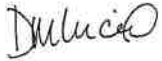
What Information Was Involved? The investigation in this matter was unable to confirm whether information related to you was actually accessed or viewed by an unauthorized actor during this event. However, Maxim Healthcare is notifying you out of an abundance of caution. The information related to you that was potentially accessible within the impacted email account includes your <<b2b_text_1(name, address, and Data Elements)>>.

What We Are Doing. We take this incident and the security of personal information in our care seriously. Upon learning of the suspicious activity, Maxim Health worked quickly to investigate and respond to this event, assess the security of relevant systems, and notify potentially affected individuals. As an immediate response, Maxim Healthcare instituted additional security protocols, including implementation of Multi-Factor Authentication for all email accounts and transitioned to a new Security Operations Center with advanced detection and response capabilities. Maxim is further committed to integrating additional cybersecurity infrastructure and security measures without negatively impacting the healthcare populations we serve. Maxim Healthcare is notifying relevant state and federal regulators.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and explanations of benefits. Any suspicious activity should be reported to the appropriate insurance company, health care provider, or financial institution. Additionally, it is recommended that you promptly change your password and security question and answer, as applicable, or take other steps appropriate to protect the potentially accessibly online account information and all other online accounts for which the same username, email address, password, and security question and answer are used. You may also review the information contained in the attached *Steps You Can Take to Protect Personal Information*.

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, please visit our website at www.maximhealthcare.com. You may also contact our call center at 1-???-???-???? Monday through Friday, 8:00 a.m. to 5:30 p.m., Central Time (excluding some U.S. holidays) or write to Maxim Healthcare's Privacy Officer at 7227 Lee Deforest Drive, Columbia MD 21046.

Sincerely,

A handwritten signature in dark ink, appearing to read "D. Lucio".

Darlene M. Lucio
Privacy Officer
Maxim Healthcare Services

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 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	1-888-397-3742	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. Maxim Healthcare Services is located at 7227 Lee Deforest Drive, Columbia, Maryland 21046.

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 1 Rhode Island resident impacted by this incident.